Escuela Politécnica Superior

Análisis y correlación entre probabilidad e impacto de los riesgos

Máster Ciber Seg

Máster Universitario en Ciberseguridad

Trabajo Fin de Máster

Autor:

Juan Santonja Lillo

Tutor/es:

José Vicente Berná Martínez

Junio 2019

Universitat d'Alacant
Universidad de Alicante

Hoja dejada en blanco intencionadamente

Resumen

El presente Trabajo Fin de Máster (TFM) plantea como objetivo principal la definición de un método que permita el cálculo objetivo del impacto en los análisis de riesgos.

Para comenzar, realizamos una introducción de la fundamentación teórica de los análisis de riesgos junto con las bases y elementos estructurales que lo componen. A continuación efectuamos un resumen de los métodos mas utilizados como son Octave, Magerit, Mehari, Cramm, NIST SP 800:30 junto con las ventajas y desventajas de cada uno de ellos.

Posteriormente, describimos la metodología de análisis de impacto en el negocio (BIA) que nos aporta una visión sobre los impactos operacionales de las organizaciones.

Con la información tanto de la metodología de riesgos como con le BIA analizamos como cada uno de ellos realiza el cálculo del impacto lo que aporta información relevante para la sistematización del cálculo.

Para finalizar, tras una pequeña descripción de antecedentes del *paper* denominado "*Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method" [32],* establecemos los criterios mínimos y formalizamos las variables que nos permiten cuantificar el impacto basado en procedimiento sistemático.

Palabras clave: Análisis de Riesgos, Calculo de Impacto, Risk Assesment

Resum

El present Treball de Fi de Màster (TFM) planteja com a objectiu principal la definició d'un mètode que permeta el càlcul objectiu de l'impacte en els anàlisis de riscos.

Per a començar, realitzem una introducció de la fonamentació teòrica dels anàlisis de riscos juntament amb les bases i elements estructurals que ho componen. A continuació efectuem un resum dels mètodes mes utilitzats com són Octave, Magerit, Mehari, Cramm, NIST SP 800:30 juntament amb els avantatges i desavantatges de cadascun d'ells.

Posteriorment, descrivim la metodologia d'anàlisi d'impacte en el negoci (BIA) que ens aporta una visió sobre els impactes operacionals de les organitzacions.

Amb la informació tant de la metodología de riscos com amb li BIA analitzem com cadascun d'ells realitza el càlcul de l'impacte el que aporta informació rellevant per a la sistematització del càlcul.

Per a finalitzar, després d'una petita descripció d'antecedents del paper denominat "*Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method* [32]", establim els criteris mínims i formalitzem les variables que ens permeten quantificar l'impacte basat en procediment sistemàtic.

Paraules clau: Anàlisi de Riscos, Càlcul d'Impacte, Risk Assesment

Motivación, justificación y objetivo general

El ámbito de la seguridad en las tecnologías de la información y el de la gestión de riesgos han sido disciplinas que han ido evolucionando a lo largo de los años desde que me incorporé al mundo laboral. Si bien el primero, ha ido de la mano de la transformación y crecimiento tecnológico, el segundo se remonta desde hace décadas en los ámbitos de proyectos y financieros.

La vertiente financiera de la gestión de riesgos es necesaria para evitar pérdidas y mejorar los márgenes de negocio de las entidades. Este caso de uso primario e inherente a dichas entidades ha favorecido que se extrapole a los ámbitos operacionales y tecnológicos entre otros. La seguridad tecnológica ha sido una de las áreas donde los análisis de riesgos se han convertido como un elemento principal para la definición de planes, políticas y controles.

Uno de los elementos catalizadores hacia la visión y cultura de riesgos fue la crisis de la década pasada, en la que se ubica el libro de Nassim Nicholas Taleb que introdujo el concepto de “cisne negro” con referencia a los riesgos de mercados financieros llamado “El cisne negro – El impacto de lo altamente improbable”.

Según Taleb, para que un evento pueda considerarse un cisne negro debe reunir tres atributos: primero, no pertenecer al reino de las expectativas normales pues nada en el pasado lleva a pensar que sea posible; segundo, que ocasione un enorme impacto; y finalmente que, una vez ocurrido, surjan explicaciones que lo hacen aparecer como predecible [1] .

Estos cisnes negros, derivados de la infravaloración del impacto y la dificultad para tener una visión holística en empresas de medio y gran tamaño, requieren una visión proactiva y cultura de riesgos maduras.

Los ingenieros de Tecnologías de la Información cuando se enfrentan a un primer análisis de riesgos requieren conocimiento técnico sobre la evaluación así como un entendimiento de como valorar las probabilidades y el impacto en caso de que materialice el riesgo.

Tener la visión probabilística y financiera no suele ser, en general, una de las características de los técnicos informáticos no relacionados con la gestión. Para solventar estas carencias, se utilizan las categorías cualitativas que facilitan el desarrollo de dichos análisis de riesgos y que en cierta medida distorsionan el cálculo final.

El objetivo del presente trabajo es establecer un procedimiento sistemático para el cálculo del impacto que no sea ambiguo y facilite la valoración de los análisis de riesgos. La variable probabilidad no forma parte del presente estudio al tener una relación directa con los eventos generados en los sistemas de gestión de alertas y *logs*.

Así mismo, la temática elegida es uno de los focos principales de los reguladores españoles y europeos. La "cultura de riesgo" se esta estableciendo en las entidades financieras como uno de los elementos principales de madurez y control frente eventos de pérdida.

Por otra parte, se está generalizando el uso de GRC (Gobernabilidad, Riesgo y Cumplimiento) que se refiere a una estrategia para administrar el gobierno general de una organización, la administración de riesgos empresariales y el cumplimiento de las regulaciones. Son un enfoque estructurado para alinear TI con los objetivos de negocio, al tiempo que gestiona eficazmente los riesgos y cumple con los requisitos de cumplimiento.

Estas estrategias vienen de la mano de herramientas específicas que cuentan con módulos de gestión de riesgos y funcionalidades "*out of the box*". Estas funcionalidades son facilidades que agilizan la parametrización, no obstante, los técnicos y programadores requieren conocimiento tanto para la parametrización de la herramienta como para la realización de análisis de riesgos en los que tuvieran que participar.

En definitiva, la gestión de riesgos se posiciona como uno de los elementos clave de gobierno y la toma de decisiones en las empresas, con lo que cualquier elemento que ayude y facilite dichos cálculos tiene una potencial funcionalidad y beneficio.

Agradecimientos

A mis hijos, Gabriela, Juan y Lucas, por haberme regalado parte de su tiempo para llevar a cabo el Master y el trabajo que hoy culmina.

A mi esposa Carol, que sin su apoyo y comprensión hubiera sido imposible compaginar todas las tareas académicas, familiares y laborales.

A mi profesor José Vicente Berná por el esfuerzo, diligencia y consejos.

No quiero dejar de agradecer a Banco Sabadell a través de su filial tecnológica SABIS que me han brindado la oportunidad de llevar a cabo el Master en Ciberseguridad en la Universidad de Alicante.

Citas

Simplemente juega. Diviértete. Disfruta el juego.

Michael Jordan

No nos atrevemos a muchas cosas porque son difíciles, pero son difíciles porque no nos atrevemos a hacerlas.

Seneca

Un hombre se le acercó a un sabio anciano y le dijo: -Me han dicho que tú eres sabio….

Por favor, dime qué cosas puede hacer un sabio que no está al alcance de las demás de las personas.

El anciano le contestó: cuando como, simplemente como;

duermo cuando estoy durmiendo, y cuando hablo contigo, sólo hablo contigo.

Pero eso también lo puedo hacer yo y no por eso soy sabio, le contestó el hombre, sorprendido.

Yo no lo creo así, le replicó el anciano.

Pues cuando duermes recuerdas los problemas que tuviste durante el día o imaginas los que podrás tener al levantarte.

Cuando comes estás planeando lo que vas a hacer más tarde.

Y mientras hablas conmigo piensas en qué vas a preguntarme o cómo vas a responderme, antes de que yo termine de hablar.

El secreto es estar consciente de lo que hacemos en el momento presente y así disfrutar cada minuto del milagro de la vida.

Cuento Budista

Índice de contenidos

Índice de figuras

Índice de tablas

1. Introducción

Dentro del ámbito financiero el análisis de riesgos ha tomado especial relevancia tras la crisis iniciada en 2008, si bien, era uno de los ámbitos en los que se trabajaba de modo sistemático en dichas entidades, la subestimación de ciertos parámetros infravaloró la exposición de los Bancos impidiendo una detección temprana de las amenazas que tenían latentes en sus activos.

En este sentido, José Manuel González-Páramo, miembro del Comité Ejecutivo del Banco Central Europeo, lo indicaba en el discurso de clausura de las X Jornadas de Política Económica de 2011, en la valoración incorrecta del riesgo en cuenta a las hipotecas subprime [2].

La situación anterior provocó un refuerzo del control interno de las empresas con foco en la gestión de riesgos. Los estamentos reguladores revisaron los procesos de control definiendo nuevas guías y reformulando leyes en el caso de organismos públicos. Un ejemplo lo podemos encontrar en las Directrices sobre la evaluación del riesgo de TIC publicado por la EBA (Autoridad Bancaria Europea). Tal como se indica en la guía en su Título 3, las autoridades competentes evaluarán si la entidad ha identificado, evaluado y mitigado adecuadamente sus riesgos de TIC. Este proceso deberá formar parte del marco de gestión del riesgo operacional y será congruente con el enfoque aplicable a este riesgo. [3]

Cada año, la Supervisión Bancaria del BCE, en colaboración con los supervisores nacionales, identifica y evalúa los riesgos que afectan a las entidades de crédito en la zona del euro. El resultado de este ejercicio sirve de base para definir las prioridades supervisoras y establecer las áreas fundamentales para el seguimiento y análisis periódicos de los riesgos a los que están expuestas las entidades supervisadas.[4]

El MUS (Mecanismo de Supervisión Único) realiza un ejercicio de análisis para determinar que áreas son de especial protección para el ejercicio.

En este sentido, los factores de riesgo más importantes identificados para 2019 son:

- Incertidumbres geopolíticas
- Préstamos dudosos (NPL) antiguos y potenciales
- Ciberdelincuencia y fallos informáticos

En la figura 1 se puede observar la distribución de riesgos por importancia para el año 2019.

Figura 1. Mapa de Riesgos del Mus para 2019

La Ciberdelincuencia y fallos informáticos se sitúa como uno de los focos de riesgos de las empresas y organismos públicos con una probabilidad alta e impacto alto en caso de materializarse. Esta es la definición de riesgo que nos guiará a lo largo del presente trabajo.

Es de vital importancia que en las empresas se establezcan objetivos empresariales y, a partir de ellos, políticas de seguridad que permitan controlar la realización de los procesos para así optimizar el análisis de riesgos. Con la implementación de este imperativo estudio en las empresas, se debería garantizar la continuidad del negocio, asegurando los principios de la seguridad de la información.

La cuantificación de la probabilidad se ha basado en la utilización de datos históricos y modelos estadísticos que se consideran correctos y ajustados. En cambio, la valoración del impacto depende de las particularidades de cada empresa puesto que los sistemas informáticos forman parte del modelo productivo del negocio. El impacto depende de una serie de variables que combinadas entre sí formulan una ecuación compleja difícil de objetivizar.

El presente trabajo se centra en revisar como se calcula el impacto tanto en los análisis de riesgos como en el BIA (Business Impact Analysis). Este último permite a empresas estimar el impacto operacional y financiero de interrupciones. Como resultado haremos una propuesta o algoritmo general de estimación que permita sistematizar el cálculo y por tanto mejorar la estimación de la exposición.

En los capítulos de “Estado del Arte”, 1, 2 y 3 revisaremos los conceptos fundamentales de Análisis de Riesgos y BIA desde una perspectiva de los parámetros utilizados en cada uno de ellos y sus fundamentos.

En el capítulo denominado “Análisis de Impacto en los modelos”, extraemos y sumarizamos el uso de la variable “Impacto” mostrando las ventajas e inconvenientes de su uso.

En el capítulo “Modelo Propuesto” estableceremos la sistematización del cálculo de la variable impacto que permita un cálculo objetivo mejorando las valoraciones cualitativas.

En los capítulos de “Conclusiones y Trabajo Futuro” resumimos los aspectos mas relevantes del trabajo de investigación y sobre que áreas podrían realizarse estudios con nivel de detalle superior.

En el siguiente punto, y para situar al lector en el contexto, se muestran los pasos generales para realizar un análisis de riesgos siguiendo las recomendaciones de INCIBE (Instituto Nacional de Seguridad) [5]

Posteriormente desarrollamos las diferentes metodologías más utilizadas y que nos servirán para obtener la información necesaria para la valoración del impacto, objetivo final del presente trabajo.

1.1. Pasos en el Análisis de Riesgos

El análisis de riesgos es uno de los trabajos más importantes a la hora de definir proyectos e iniciativas para la mejora de la seguridad de la información en las empresas y organizaciones.

El plan director de seguridad vendrá de la mano de un análisis de riesgos previo que ayudará a centrar las áreas de mejora con respecto a las debilidades de seguridad.

Las fases o etapas que componen un análisis de riesgos dependen de la metodología escogida. Siguiendo el criterio de INCIBE se ha seleccionado un conjunto de fases que son comunes en la mayor parte de las metodologías para el análisis de riesgos para poder entender conceptualmente el procedimiento como se puede ver en la figura 2.

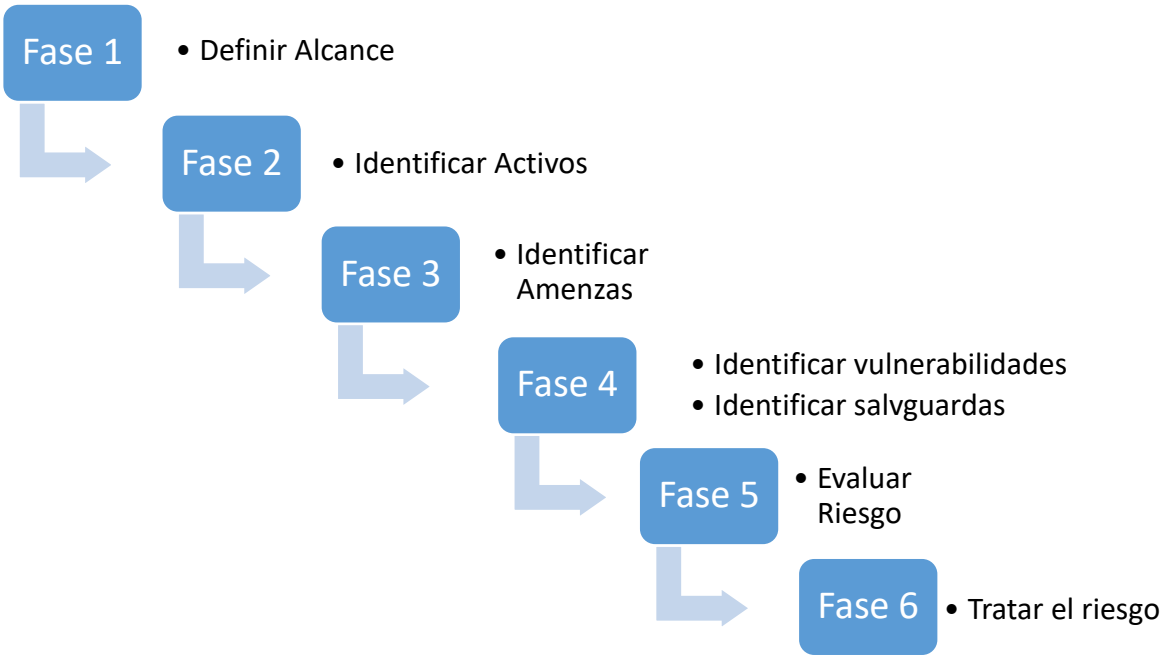

Figura 2. Pasos de Análisis de Riesgos

Fase 1. Definir el alcance

El primer paso a la hora de llevar a cabo el análisis de riesgos, es establecer el alcance del estudio. Han de seleccionarse las áreas estratégicas sobre las que mejorar la seguridad. Es posible definir un alcance más limitado atendiendo a departamentos, procesos o sistemas. Por ejemplo, análisis de riesgos sobre los procesos del departamento Administración, análisis de riesgos sobre los procesos de producción y gestión de almacén o análisis de riesgos sobre los sistemas TIC relacionados con la página web de la empresa, etc.

Fase 2. Identificar los activos

Una vez definido el alcance, se debe identificar los activos más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio. Para mantener un inventario de activos sencillo puede ser suficiente con hacer uso de una hoja de cálculo o tabla.

Fase 3. Identificar / seleccionar las amenazas

Una vez identificados los principales activos, el siguiente paso consiste en identificar las amenazas a las que estos están expuestos. El conjunto de amenazas es amplio y diverso por lo que se debe hacer un esfuerzo en mantener un enfoque práctico y aplicado. Por ejemplo, si la intención es evaluar el riesgo que se corre frente a la destrucción de un servidor de ficheros, es

conveniente, considerar las averías del servidor, la posibilidad de daños por agua (rotura de una cañería) o los daños por fuego, en lugar de plantearse el riesgo de que el CPD sea destruido por un meteorito.

A la hora de identificar las amenazas, puede ser útil tomar como punto de partida el catálogo de amenazas que incluye la metodología MAGERIT v3 [6].

Fase 4. Identificar vulnerabilidades y salvaguardas

La siguiente fase consiste en estudiar las características de los activos para identificar puntos débiles o vulnerabilidades. Por ejemplo, una posible vulnerabilidad puede ser identificar un conjunto de ordenadores o servidores cuyos sistemas antivirus no están actualizados o una serie de activos para los que no existe soporte ni mantenimiento por parte del fabricante. Posteriormente, a la hora de evaluar el riesgo se aplicarán penalizaciones para reflejar las vulnerabilidades identificadas.

Por otra parte, también se analizará y documentarán as medidas de seguridad implantadas en la organización. Por ejemplo, es posible que se haya instalado un sistema SAI (Sistema de Alimentación Ininterrumpida) o un grupo electrógeno para abastecer de electricidad a los equipos del CPD. Ambas medidas de seguridad (también conocidas como salvaguardas) contribuyen a reducir el riesgo de las amenazas relacionadas con el corte de suministro eléctrico.

Estas consideraciones (vulnerabilidades y salvaguardas) se deben tener en cuenta cuando se vaya a estimar la probabilidad y el impacto.

Fase 5. Evaluar el riesgo

En esta fase se dispone de los siguientes elementos:

- Inventario de activos.
- Conjunto de amenazas a las que está expuesta cada activo.
- Conjunto de vulnerabilidades asociadas a cada activo
- Conjunto de medidas de seguridad implantadas

Con esta información, ya podemos calcular el riesgo. Para cada par activo-amenaza, se estima la probabilidad de que la amenaza se materialice y el impacto sobre el negocio que esto produciría. El cálculo de riesgo se puede realizar usando tanto criterios cuantitativos como cualitativos

La cuantificación del riesgo desde la vertiente cuantitativa es la que permitirá realizar un cálculo del impacto objetivo y que será desarrollada en las fases posteriores del presente documento. Dicho cálculo se realiza del siguiente modo:

RIESGO = PROBABILIDAD x IMPACTO.

Fase 6. Tratar el riesgo

Una vez calculado el riesgo, se debe tratar los riesgos que superen un límite que se haya establecido por la organización. A la hora de tratar el riesgo, existen cuatro estrategias principales:

- **Transferir** el riesgo a un tercero. Por ejemplo, contratando un seguro que cubra los daños a terceros ocasionados por fugas de información.
- **Eliminar** el riesgo. Por ejemplo, eliminando un proceso o sistema que está sujeto a un riesgo elevado. En el caso práctico que hemos expuesto, podríamos eliminar la wifi de cortesía para dar servicio a los clientes si no es estrictamente necesario.
- **Asumir** el riesgo, siempre justificadamente. Por ejemplo, el coste de instalar un grupo electrógeno puede ser demasiado alto y por tanto, la organización puede optar por asumir.
- **Implantar** medidas para mitigarlo. Por ejemplo, contratando un acceso a internet de respaldo para poder acceder a los servicios en la nube en caso de que la línea principal haya caído

2. Análisis de Riesgos

El precepto fundamental de la seguridad de la información es apoyar la misión de la organización. Todas las empresas están expuestas a incertidumbres, algunas de las cuales afectan a la organización de manera negativa.

Para respaldar a la organización, los profesionales de seguridad de TI deben poder ayudar a los gestores de sus organizaciones a comprender y gestionar estas incertidumbres. Gestionar las incertidumbres no es una tarea fácil, los recursos limitados y un panorama cambiante de amenazas y vulnerabilidades hacen que mitigar por completo todos los riesgos sea de gran dificultad.

Por lo tanto, los profesionales de la seguridad de TI deben tener un conjunto de herramientas que les ayude a compartir una visión común con dirección del negocio con respecto al impacto potencial de las amenazas relacionadas con la seguridad de la información. [7]

Este conjunto de herramientas y técnicas deben ser coherentes, repetibles, rentables y reducir los riesgos a un nivel razonable.

El concepto de riesgo y evaluación de riesgo tiene una larga historia. Hace más de 2400 años, los atenienses ofrecieron su capacidad de evaluar el riesgo antes de tomar decisiones. Sin embargo, la evaluación de riesgos y la gestión de riesgos como campo científico son relativamente jóvenes, no tienen más de 30 a 40 años. A partir de este período, vemos las primeras revistas científicas, artículos y conferencias que cubren ideas y principios fundamentales sobre cómo evaluar y gestionar adecuadamente el riesgo.[8]

El Análisis de riesgos consiste no sólo en una observación detallada y sistemática, sino que principalmente es una propuesta metodológica que permite el conocimiento de los riesgos y sus fuentes o causas (peligros) , las consecuencias potenciales y remanentes, y la probabilidad de que esto se presente. [9]

Existen muchas herramientas y técnicas disponibles para administrar los riesgos de las organizaciones. Algunas de estás técnicas se desarrollan en formato reducido en el presente trabajo.

Existen un gran número de trabajos y publicaciones relacionados sobre análisis de riesgos, así en el artículo "*Methods and models in process safety and risk management: Past, present and*

future" [10] se realiza un estudio sistemático e la literatura en el que se identifican documentos que reflejan la evolución de los procesos de análisis,

En dicho documento se identifican tanto el número de publicaciones por décadas como una tipificación de los trabajos realizados en función de la tipología de riesgos. En la figura 3 se pude observar dicha información.

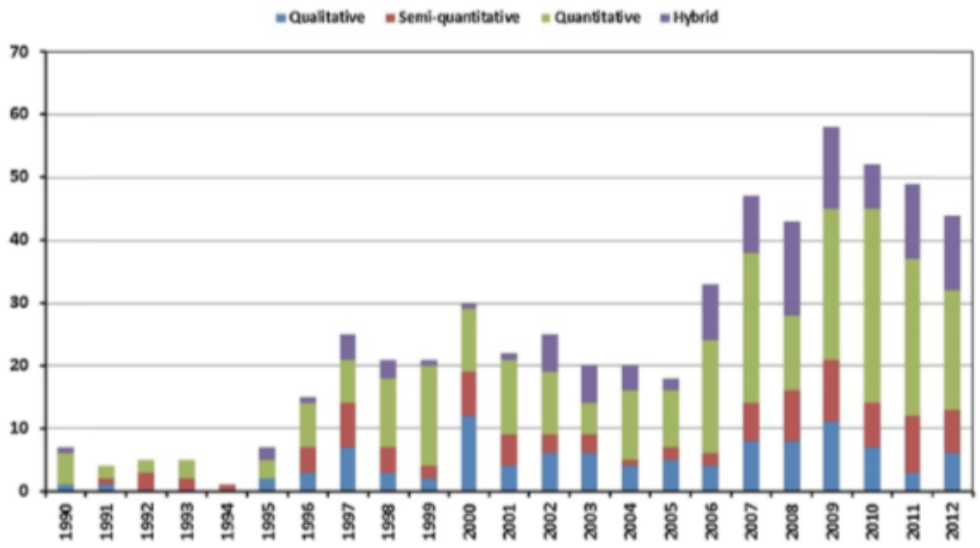

Figura 3. Número de Publicaciones por tipo

El número de trabajos ha ido creciendo considerablemente durante los últimos años, en las diferentes categorías; Cualitativo, Semi-Cuantitativo, Cuantitativo e Hibrido.

El análisis cualitativo se refiere a representaciones no numéricas y explicaciones basadas en atributos gráficos, diagramas de flujo y fuentes de datos.

Los análisis semi-cuantitativos se encuentran entre el cualitativo y cuantitativo dando como resultado valoraciones aproximadas en lugar de exactas o absolutas. Estos métodos son útiles cuando no se puede realizar mediciones o valoraciones directas y se acepta la posibilidad de realizar inferencias.

El análisis cuantitativo proporciona una estimación numérica realista lo que facilita una mejor comprensión y una toma de decisiones basada en hechos objetivos. En el artículo "*How Useful Is Quantitative Risk Assessment*?" [11] se discute el uso de la evaluación cuantitativa de riesgos en la toma de decisiones con respecto a la seguridad de sistemas tecnológicos complejos. Las ideas obtenidas se comparan con las de los métodos de seguridad tradicionales y se argumenta que los dos enfoques se complementan entre sí. También, se pueden encontrar ejemplos de

aplicaciones en energía nuclear, sistemas espaciales y un incinerador de agentes químicos para demostrar los beneficios prácticos del análisis cuantitativo.

El análisis híbrido es simplemente una combinación de análisis cuantitativo y cualitativo. Se diferencia del semi-cuantitativo porque los métodos híbridos proporcionan resultados cuantitativos más precisos y realistas a través de su análisis cuantitativo. Además, se observa que cada análisis semi-cuantitativo puede no incluir una parte cualitativa; en su lugar, se puede utilizar sólo una cuantificación simple. Por lo tanto, el análisis híbrido proporciona un análisis exhaustivo de la seguridad del proceso y la evaluación de riesgos.

Los métodos de análisis cuantitativo y cualitativo son dos métodos fundamentales que se utilizan para el análisis de exposición de los activos frente a los riesgos. Pero existen algunas desventajas para los métodos de evaluación de riesgos de la información (ver Tabla 1) . [12]

Métodos Cuantitativos	
Ventajas	• Permite la definición de las consecuencias de un modo cuantitativo. • Permiten el análisis de beneficio/coste durante la selección de las salvaguardas. • Se obtiene una imagen mas ajustada de la valoración de riesgos.
Desventajas	• Las medidas cuantitativas dependen del alcance y exactitud de las escalas de medida. • El resultado del análisis puede ser no preciso y a veces confuso. • Debe ser enriquecido con una descripción cualitativa. • Suelen ser mas caros y requieren de mayor experiencia.
Ventajas	• Permite determinar grandes áreas de riesgos en un corto periodo de tiempo y sin mucha experiencia. • Suelen ser análisis mas fáciles y económicos.
Desventajas	• No permite la estimación de probabilidades y resultados utilizando medidas numéricas.

	• El análisis de coste/beneficio es mas difícil durante la fase de determinación de las salvaguardas. • Los resultados son de carácter general mediante aproximaciones.

Tabla 1 Ventajas y Desventajas de métodos Cuantitativos y Cualitativos

Los enfoques anteriores se ven reflejados en los diferentes estándares conocidos comúnmente como Frameworks o Marcos de Trabajo de Riesgos. Entre los marcos de gestión de riesgos de TI más conocidos se encuentran los siguientes: NIST , Isaca IT Risk, Risk IT, Octave y Magerit entre otros. El objetivo de estos marcos es el de integrar buenas prácticas mundialmente reconocidas de forma ordenada y sistemática. Estos marcos están diseñados para facilitar el análisis de riesgos y orientan en la implantación de un sistema de gestión de riesgos [13].

Para el presente trabajo detallaremos Octave, MEHARI, MAGERIT, CRAMM, EBIOS y NIST SP 800-30, las cuales se orientan hacia el mismo objetivo, pero tienen características propias que las hacen atractivas para las empresas en todos los sectores [14].

Estas metodologías cuentan con una serie de fases, comunes o no entre ellas, que se puede observar en la Tabla 2. La elección de una ellas dependerá del criterio del analista, experiencia o sector empresarial de la organización en el que se realizará el análisis de riesgos.

Fases	**Metodologías**							
	1	1ª	1B	2	3	4	5	6
Caracterización del Sistema	X	X	X	X	X	X	X	X
Identificación de Amenazas	X	X	X		X	X	X	X
Identificación de Vulnerabilidades	X		X			X		X
Análisis de Controles	X	X	X	X	X		X	X
Determinación de la Probabilidad								X
Análisis de Impacto								X
Determinación del Riesgo	X	X	X	X	X	X		X
Recomendaciones de Control	X	X	X	X		X	X	X
Documentación de los resultados	X			X				X
Establecimiento de Parámetros			X		X			

Necesidades de Seguridad	X					X	X	

Tabla 2. Fases de las Metodologías
(1)OCTAVE (1A)OCTAVE S (1B) OCTAVE ALLEGRO, (2) MEHARI,
(3) MAGERIT, (4) CRAMM, (5) EBIOS, (6) NIST SP 800 – 30

2.1 Octave

Es una metodología para identificar y evaluar los riesgos de seguridad de la información. Está destinada a ayudar a las organizaciones a:

- Desarrollar criterios de evaluación de riesgos cualitativos que describan el riesgo operacional y la tolerancia al mismo.
- Identificar los activos que son importantes para el desarrollo de función de la organización
- Identificar vulnerabilidades y amenazas a esos activos.
- Determinar y evaluar las posibles consecuencias para la organización si se materializan alguna de las amenazas identificadas.

El marco conceptual que formó la base del enfoque original de OCTAVE fue publicado por el SEI (Software Engineering Institute) en la Universidad Carnegie Mellon en 1999. Trabajando conjuntamente con el Centro de Investigación de Telemedicina y Tecnología Avanzada (TATRC), el SEI desarrolló la metodología OCTAVE para abordar los desafíos de cumplimiento de seguridad que se enfrentaba el departamento de defensa de los EE. UU.

Desde que apareció por primera vez en septiembre de 1999, ha habido una serie de actualizaciones y cambios sobre la propia metodología que se pueden ver en la Tabla 3.

Fecha	Título de la Publicación
Septiembre 1999	OCTAVE Framework Versión 1.0
Septiembre 2001	OCTAVE Framework Versión 2.0
Diciembre 2001	OCTAVE Criteria Versión 2.0
Septiembre 2003	OCTAVE-S v0.9
Marzo 2005	OCTAVE-S v1.0
Junio 2007	Introducción de OCTAVE Allegro v1.0

Tabla 3. Actualizaciones Octave

2.1.1 Método OCTAVE

En el presente trabajo de describen tres metodologías distintas de que se encuentran disponibles para uso público: el método OCTAVE, OCTAVE-S y OCTAVE Allegro.

Cada método OCTAVE tiene una amplia aplicabilidad y la elección de uno de los métodos dependerá del enfoque que mejor se adapte a las necesidades particulares de evaluación de riesgos de seguridad de la información que el usuario determine. OCTAVE Allegro, por ejemplo, es una variante que proporciona un proceso simplificado centrado sobre los activos de información.

La versión inicial de Octave que fue consistente definía una guía de implementación de elementos relacionados con procedimientos, orientación de desarrollo, hojas de trabajo, catálogos de información y capacitación. El desarrollo se realizaba mediante una serie de talleres en los que participaba un equipo de análisis interdisciplinario extraído de unidades de negocio de toda la organización (dirección, responsables de operaciones y el personal de negocio) y miembros del departamento de TI[15].

OCTAVE esta dirigido a empresas de medio y gran tamaño con un número de empleados superior a 300 y que cumplen una serie de características:

- Organigrama de varios niveles
- Disponen de su propia infraestructura TI
- Tienen capacidad para evaluar vulnerabilidades.
- Tienen la capacidad de interpretar los resultados de las evaluaciones de vulnerabilidades.

La metodología OCTAVE cuenta con tres fases. En la fase 1, el equipo de análisis identifica los activos importantes que están destinados al tratamiento de información y la estrategia de protección actual sobre esos activos. Posteriormente determina sobre los activos identificados los más críticos para el éxito de la organización, documenta los requisitos de seguridad e identifica amenazas que pueden interferir con el cumplimiento de esos requerimientos. En la fase 2, el equipo de análisis realiza una evaluación de la infraestructura para complementar el análisis de amenazas realizado en la fase 1 e informar las decisiones de mitigación en fase 3. Finalmente, en la fase 3, el equipo de análisis realiza actividades de identificación de riesgos y desarrolla un plan de mitigación de riesgos para los activos críticos.

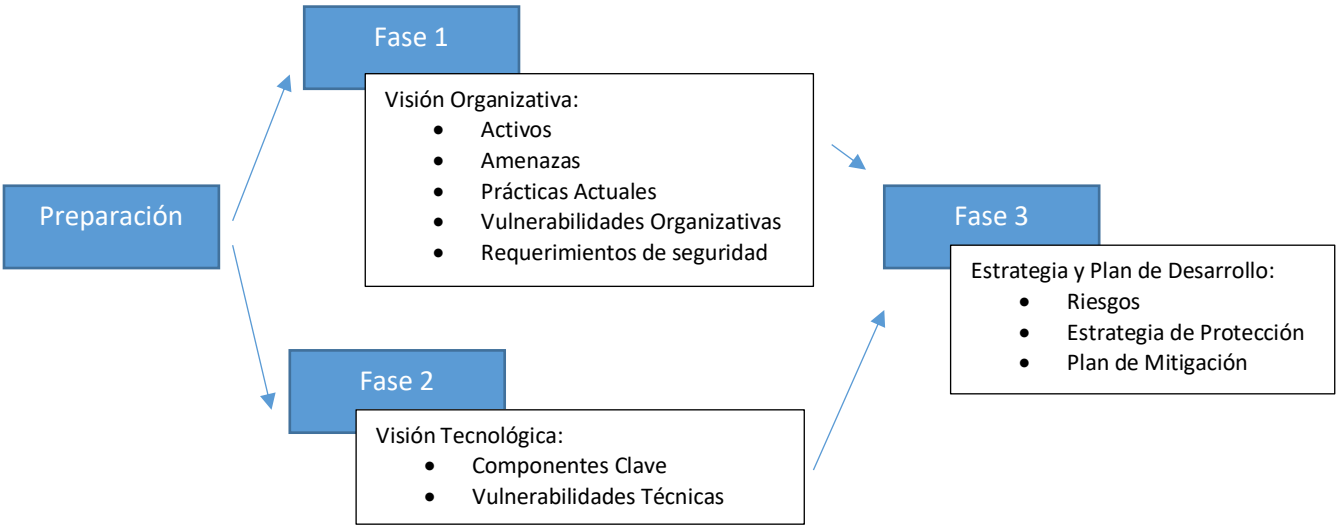

Figura 4. Fases de Octave

Octave-S fue un desarrollo de SEI para adaptarlo a empresas manufactureras de pequeño tamaño. La versión 1.0 de la metodología esta diseñada para organizaciones de alrededor 100 personas o menos.

De acuerdo con los criterios de OCTAVE, el enfoque de OCTAVE-S consta de tres fases muy similares, sin embargo, OCTAVE-S se desarrolla por un equipo de análisis que tiene un amplio conocimiento de la organización, no basándose en talleres formales de obtención de conocimientos para reunir información. Supone que el equipo de análisis (que generalmente consta de tres a cinco personas) tiene conocimiento práctico de los activos importantes relacionados con la información, los requisitos de seguridad, amenazas y prácticas de seguridad de la organización.

Otra diferencia significativa en OCTAVE-S es que está más estructurado que el método OCTAVE. Los conceptos de seguridad están incorporados en las hojas de trabajo y la guía de OCTAVE-S, lo que permite que se requieran menos profesionales experimentados en riesgos y seguridad para para desarrollar el método

Una última característica distintiva de OCTAVE-S es que requiere un examen menos extenso de la infraestructura de información de la organización. Porque , en general, las pequeñas organizaciones puede que no tenga los recursos necesarios para disponer de herramientas de vulnerabilidades, OCTAVE-S fue diseñado para incluir un examen acotado de los riesgos de infraestructura para eliminar limitaciones en la adopción por parte de este tipo de empresas.

El enfoque de OCTAVE permite la evaluación del entorno de riesgo operacional de una organización con el objetivo de obtener resultados sólidos sin la necesidad de un extenso

conocimiento de evaluación de riesgos. Este enfoque difiere de los enfoques OCTAVE anteriores al centrarse en los activos de información en el contexto de cómo se utilizan, dónde se almacenan, transportan y procesan, y como están expuestos a amenazas, vulnerabilidades e interrupciones.

Al igual que los métodos anteriores, OCTAVE Allegro se puede realizar en un entorno de colaboración, estilo taller, y contempla elementos como guías, hojas de trabajo y cuestionarios.

OCTAVE Allegro también es adecuado para el desarrollo de análisis de riesgos en organizaciones en las que no se cuenta con la experiencia suficiente en la gestión, cultura e información de riesgos.

El enfoque Allegro de OCTAVE consta de ocho pasos, como se ilustra en la Figura 5. En la fase 1, la organización desarrolla criterios de medición de riesgo coherentes con los *drivers* organizativos. Durante la segunda fase, los activos de información que se determinan como críticos se perfilan. Este proceso de perfilado establece límites claros para el activo, identifica los requerimientos de seguridad, y determina todas las ubicaciones donde el activo se almacena, transporta o procesa. En la fase 3, se identifican las amenazas en el contexto de las ubicaciones donde se almacena, transporta o procesa el activo. En la fase final, se realiza el desarrollo de enfoques de mitigación.

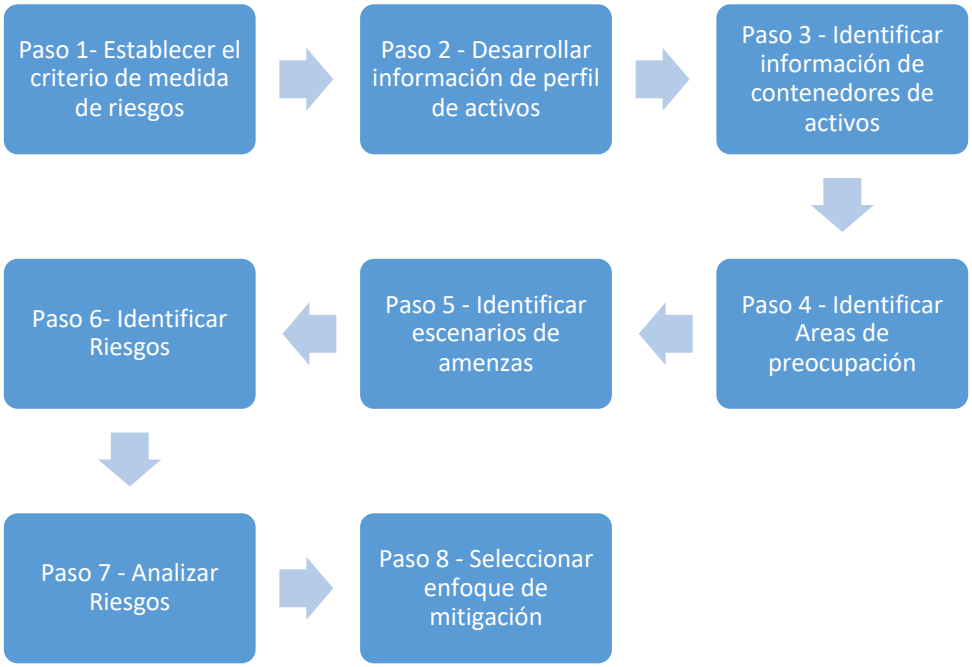

Figura 5. Fases OCTAVE Allegro

2.1. Mehari (Method for Harmonized Analysis of Risk)

Mehari es una metodología desarrollada por CUSIF (*Club De La Sécurité De L'information Français)* en 1998 que lo hizo *Open Source* en 2007.

MEHARI es un método de análisis y gestión de riesgos que también incluye, directamente, muchas fórmulas para la evaluación directa de riesgos y la selección de formas de reducirlos.

Una de las ventajas que se indican es su facilidad de uso [16] . La metodología cuenta con libros de trabajo que permiten la calificación y cuantificación de todos los elementos de riesgo.

Tal como se indica en el documento de CLUSIF [17] el primer objetivo de MEHARI es proporcionar un método para la evaluación y gestión de riesgos, concretamente en el dominio de la seguridad de la información, conforme a los requerimientos de ISO/IEC 27005:2008, proporcionando el conjunto de herramientas y elementos necesarios para su implementación.

Otros objetivos adicionales son:

- Permitir un análisis directo e individual de situaciones de riesgos descritas en los escenarios,
- Proporcionar un completo conjunto de herramientas específicamente diseñadas para la gestión de la seguridad a corto, medio y largo plazo, adaptables a diferentes niveles de madurez y tipos de acciones consideradas.

La metodología ayuda a los responsables de seguridad, responsables generales u otras personas implicadas en la gestión de riesgos, en sus diferentes actividades.

El primer ámbito, relacionado con el análisis o evaluación de riesgos propone un enfoque estructurado que se basa en los siguientes principios y factores:

- Factores estructurales (u organizacionales), los cuales no dependen de medidas de seguridad, sino de la actividad principal de la organización, su entorno y su contexto.
- Factores de reducción del riesgo, que son una función directa de las medidas de seguridad implementadas.

El análisis de la seguridad es necesario para determinar el nivel máximo de gravedad como consecuencia de una situación de riesgo. Esto es típicamente un factor estructural, mientras que la evaluación de la seguridad se utilizará para evaluar los factores de reducción del riesgo.

MEHARI permite la evaluación cualitativa y cuantitativa de esos factores, y colabora en la evaluación de los niveles de riesgo como consecuencia de ello. MEHARI integra herramientas (como criterios de evaluación, fórmulas, etc.) y bases de datos de conocimiento (en particular para el diagnóstico de las medidas de seguridad), que son un complemento esencial al marco mínimo propuesto por la ISO/IEC 27005.

El segundo ámbito, relacionado con las Evaluaciones de la seguridad, permite valorar el nivel de seguridad calidad de los mecanismos y soluciones encaminadas a la reducción del riesgo, los aspectos que contempla son:

- Revisión de vulnerabilidades, un elemento de análisis de riesgos: El resultado de la evaluación de la vulnerabilidad será, por lo tanto, una entrada fundamental para el análisis de riesgos, con el fin de garantizar que los servicios de seguridad cumplen realmente su cometido.
- Planes de seguridad basados en la revisión de vulnerabilidades. Un posible enfoque es la confección de planes de seguridad como resultado directo de la evaluación del estado de los servicios de seguridad. El proceso de gestión de la seguridad siguiendo este enfoque consiste en ejecutar una evaluación y decidir mejorar todos aquellos servicios que no tienen un suficiente nivel de calidad.
- Apoyo de las bases de datos de conocimiento en la creación de un marco de referencia de seguridad. Las bases de datos de conocimiento de MEHARI se pueden utilizar directamente para crear un marco de referencia de seguridad (o políticas de seguridad) que contendrá, y describirá, el conjunto de reglas e instrucciones de seguridad que debe seguir la empresa u organización.
- Dominios cubiertos por el modulo de evaluación de vulnerabilidades. Desde un punto de vista de análisis de riesgos, en base a la identificación de todas las situaciones de riesgo y con el deseo de cubrir todos aquellos riesgos inaceptables, MEHARI no se limita simplemente al dominio IT.
- Descripción general del modulo de evaluación. El único punto a tener en cuenta sobre el módulo de evaluación de vulnerabilidades es que proporciona una visión amplia y coherente de la seguridad.

El tercer ámbito es el análisis de amenazas la comprensión de las amenazas al negocio es fundamental, y que el análisis del contexto de seguridad merece un nivel prioritario y un método estricto y riguroso de evaluación.

Los diferentes módulos o aspectos que trata la metodología son:

- Análisis de las amenazas son la base para un análisis de riesgos. Este modulo es la clave en un análisis de riesgos. Sin un acuerdo común sobre las consecuencias de potenciales de los diferentes malfuncionamientos no es posible ningún juicio sobre los niveles de riesgo identificados.
- El análisis de las amenazas de seguridad: se requiere el análisis de amenazas para la puesta en marcha de cualquier tipo de plan de seguridad. Sin importar el enfoque utilizado, en algún punto se determinarán los medios necesarios para la implantación de los planes de acción que requerirán justificación de las inversiones necesarias.
- Clasificación: es un elemento esencial para las políticas de seguridad. Las empresas que gestionan la seguridad a través de un conjunto de reglas se encuentran obligadas a diferenciar entre las reglas internas propias y entre las acciones que se tienen que implementar en función de la sensibilidad de la información procesada.
- Acciones sobre las amenazas de seguridad: Son el fundamento de la planificación de la seguridad. El propio proceso de análisis de las amenazas de seguridad requieren de la contribución de los responsables de operación.

Las fases, desde una perspectiva general, se pueden observar en la figura 6.

Figura 6. Perspectiva MEHARI

2.2. Magerit

Esta metodología fue elaborada por el Consejo Superior de Administración Electrónica, publicando su primera versión en 1997, con un enfoque hacia los riesgos fundamentales en materia de sistemas de información.

La segunda versión fue publicada en 2005 con el fin de realizar una revisión constructiva con respecto a los riesgos de las compañías, involucrando cuestiones más profundas a cerca de la gestión de riesgos.

La tercera versión y ultima busca una nueva adaptación, teniendo en cuenta no solo la experiencia práctica sino también la evolución de las normas internacionales de ISO que constituyen un referente.

De acuerdo al documento de metodología MAGERIT el análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
2. determinar a qué amenazas están expuestos aquellos activos
3. determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
4. estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
5. estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza

La siguiente figura recoge esta visión de un modo resumido:

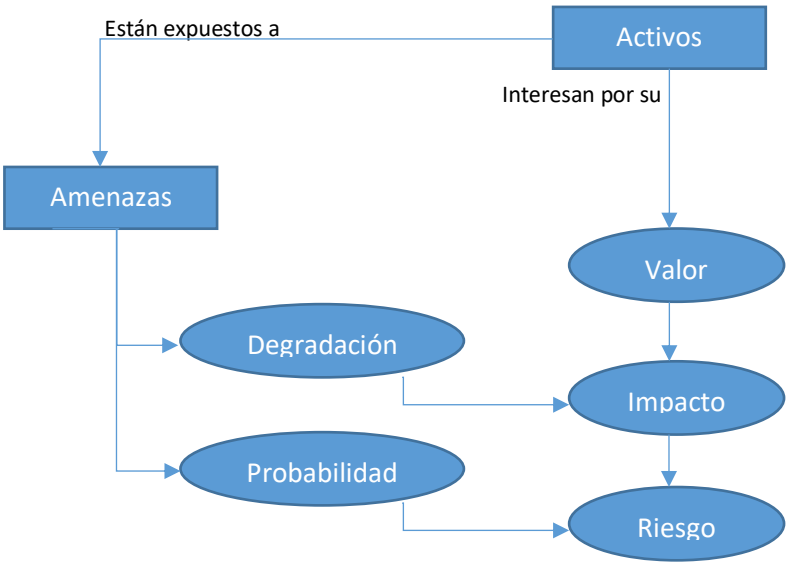

Figura 7. Visión MAGERIT

El método de análisis de riesgos cuenta con varios pasos esenciales relacionados con los activos, amenazas, salvaguardas, impacto residual y riesgo residual que se resumen a continuación.

En el paso 1, relacionado con los activos son los componente o funcionalidades de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones, equipos , comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

En esta fase se cataloga e identifica, principalmente, el valor del activo para la organización. Para ello se tienen en cuenta aspectos como si el sistema maneja y los servicios que se prestan (activos denominados esenciales) maneja información vital o crítica para el negocio. En este sentido se tienen en cuenta dimensiones que calibran el nivel de confidencialidad, integridad, disponibilidad , autenticidad y trazabilidad. Otro aspecto relacionado con la valoración a tener cuenta, es la disponibilidad, que puede tener un impacto mas complejo de medir relacionado con la interrupción del servicio o negocio.

El paso 2, consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño.

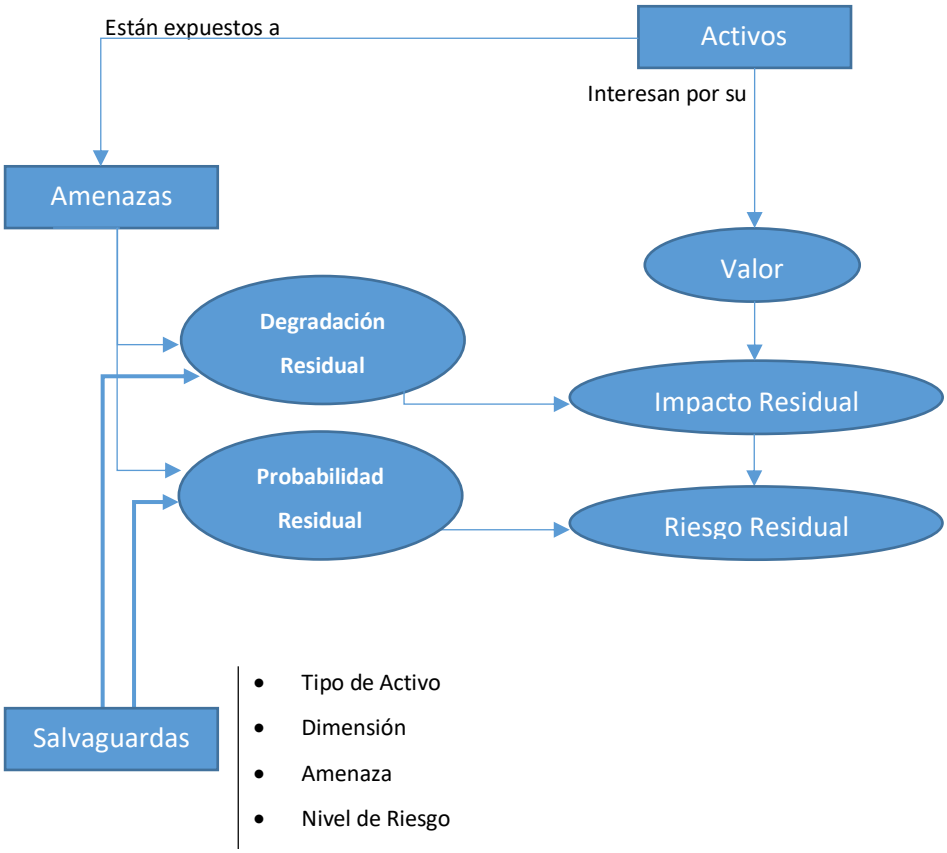

Figura 8. Elementos de Análisis MAGERIT

Para ello hay que tener en cuenta la identificación de las amenazas y la valoración del impacto de las mismas. Tanto la probabilidad como el impacto se determinan en esta fase, conformando el riesgo inherente, tal como se definido en la sección inicial de presente trabajo.

En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto. En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otra seguridad física y, por último, está la política de personal.

Por tanto el paso 3, se encarga de identificar las salvaguardas y la eficacia de la protección sobre los activos.

En el paso 4, Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que se ha modificado el impacto, desde un valor potencial a un valor residual.

El cálculo del impacto residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación.

La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

El paso 5, dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual.

El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la probabilidad de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia.

La magnitud de la degradación se toma en consideración en el cálculo del impacto residual.

La magnitud de la probabilidad residual tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

2.3. Cramm

CRAMM (CCTA Risk Analysis and Management Method), es el método de análisis y control de riesgos de la Central Computer and Telecommunications Agency (CCTA) del gobierno británico, permite identificar, medir y reducir al mínimo los ataques a los que están expuestas las organizaciones día a día y es definida como una metodología que aplica los conceptos de manera formal, estructurada y disciplinada protegiendo los principios de seguridad de la información de un sistema y de sus activos.

Cabe resaltar que CRAMM realiza un análisis de riesgos cualitativo y cuantitativo por lo que se conoce como una metodología mixta, ésta se apoya de una herramienta de gestión, lo que

permite a las organizaciones tener una visión clara y prioriza da de las amenazas a las que está expuesta y que pueden afectar los recursos y la continuidad del negocio, basándose en una matriz donde las filas representan los activos y las columnas los riesgos que podrían afectar la integridad, disponibilidad y confidencialidad de los mismos , por otro lado, CRAMM proporciona información acerca de las características de funcionamiento del sistema y una identificación profunda y clara de los activos que se encuentran más expuestos.

Los elementos que se deben tener en cuenta para realizar un adecuado análisis de riesgos con la metodología CRAMM son: activos, vulnerabilidades, riesgos, amenazas, contramedidas, implementación y auditoría, los cuales permiten obtener un mejor resultado y asegurar la continuidad de negocio.[14]

Su versión inicial data de 1987 y la versión vigente es la 5.2, tiene un alto calado en administración pública británica, pero también en empresas e instituciones de gran tamaño. Dispone de un amplio reconocimiento [18]

La metodología de CRAMM incluye las siguientes 3 etapas, que se pueden ver en la figura:

- La primera de las etapas recoge la definición global de los objetivos de seguridad entre los que se encuentra la definición del alcance, la identificación y evaluación de los activos físicos y software implicados, la determinación del valor de los datos en cuanto a impacto en el negocio y la identificación.
- En la segunda etapa de la metodología se hace el análisis de riesgos, identificando las amenazas que afecta al sistema, así como las vulnerabilidades que explotan dichas amenazas y por último el cálculo de los riesgos de materialización de las mismas.
- En la tercera etapa se identifican y seleccionan las medidas de seguridad aplicadas en la entidad obteniendo los riesgos residuales, CRAMM proporciona una librería de unas 3000 medidas de seguridad.

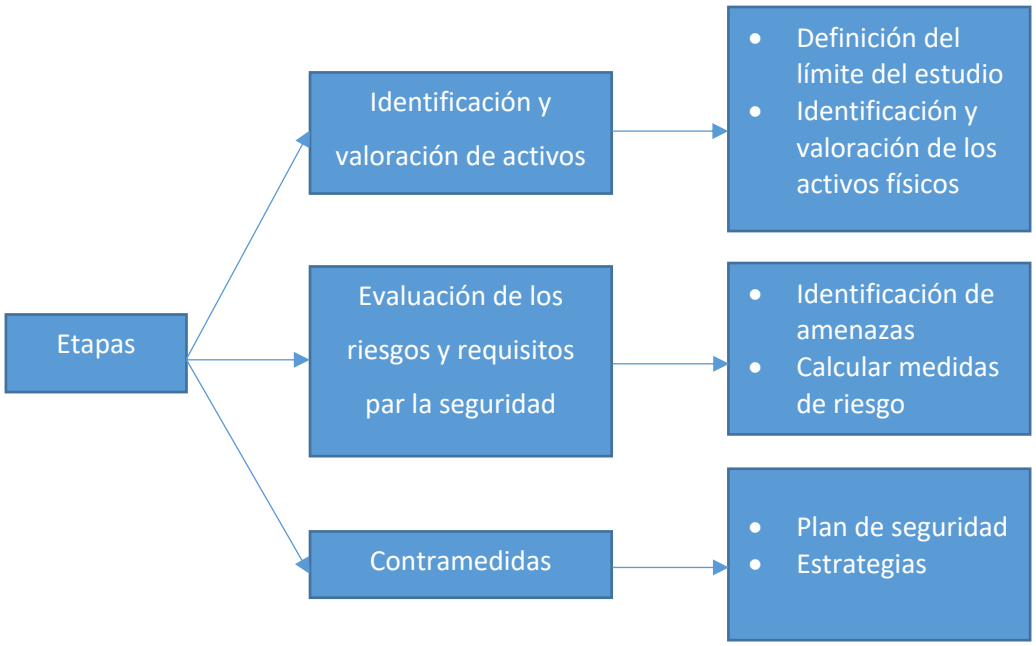

Figura 9. Etapas de CRAMM

CRAMM permite identificar hardware, software, datos y activos de localización que componen el sistema de información. Los activos físicos se valoran en función del coste que supone su remplazo, los datos e información se cuantifican en función del impacto que supone la indisponibilidad, destrucción, divulgación o modificación de la misma.[19]

El estándar clasifica los activos como software y hardware mediante su valor, sensibilidad y criticidad en la organización. En el primero de ellos, tiene en cuenta las aplicaciones, los sistemas y los datos de la organización. En el segundo, el hardware, se considera toda la infraestructura física de la organización.

La evaluación de las vulnerabilidades se realiza de un modo sistemático y estructurado mediante el análisis de software, hardware, aspectos físicos, ambientales y humanos. Como las metodologías anteriores, se pueden utilizar dos métodos para determinar las vulnerabilidades:

- Método Cualitativo: mediante *Brain Storming*, entrevistas con expertos, foros y debates de los involucrados en el proceso.
- Método Cuantitativo: mediante la determinación de probabilidades de ocurrencia.

Las probabilidades, se determinan mediante la frecuencia de aparición de un determinado evento en la organización, calculando el riesgo con la magnitud del impacto por la probabilidad de la amenaza.

La combinación anterior, de la valoración de los activos junto con los niveles de amenazas y vulnerabilidades da como resultado una ponderación del riesgo en una escala del 1 al 7 considerando el 1 como el nivel mas bajo y el 7 como el nivel mas alto.

2.4. Nist SP 800:30

SP 800:30 (Guía de Gestión de Riesgos de los Sistemas de Tecnología de la Información) [20]. Es un estándar desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST), fue formulado para la evaluación de riesgos de seguridad de la información especialmente a los sistemas de TI, proporciona una guía para la seguridad de las infraestructuras de la misma desde una perspectiva técnica [21].

Por otro lado, esta guía provee fundamentos para la administración de riesgos así como la evaluación y mitigación de los riesgos identificados dentro del sistema de TI con el objetivo de apoyar a las organizaciones con todo lo relacionado a Tecnología.

La metodología NIST SP 800:30 está compuesta por nueve fases, identificadas las principales en la figura 10, y que se definen como:

- caracterización del sistema, la cual permite establecer el alcance y los límites operacionales de la evaluación de riesgos en la empresa;
- identificación de amenazas, es donde se definen las fuentes de motivación de las mismas;
- identificación de vulnerabilidades, en esta fase desarrolla una lista de defectos o debilidades del sistema que podrían ser explotadas por una amenaza;
- análisis de controles;
- determinación de la probabilidad;
- análisis de impacto;
- fase de determinación del riesgo, ayuda a evaluar el riesgo en el sistema de información
- recomendaciones de control en donde se proporcionan los controles que podrían mitigar el riesgo identificado disminuyéndolo hasta un nivel aceptable, finalmente

está la documentación de resultados la cual genera un informe con la descripción de amenazas y vulnerabilidades, midiendo el riesgo y generando recomendaciones para la implementación de controles.

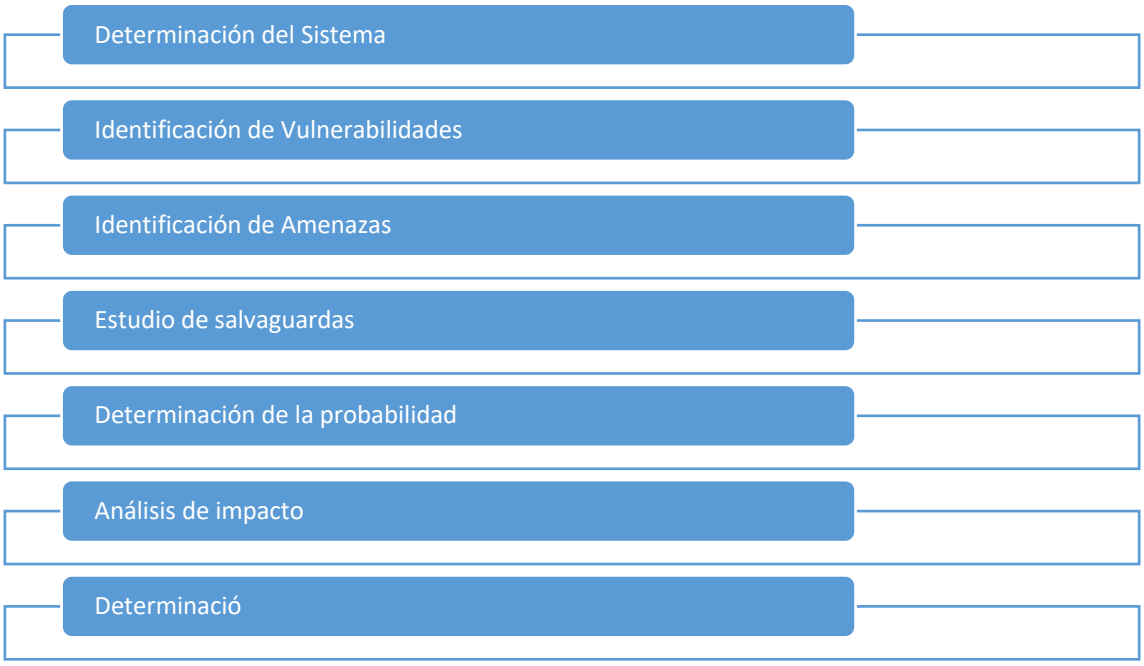

Figura 10 - Fases SP 800:30

Esta metodología proporciona una base para el desarrollo efectivo del programa de gestión de riesgos que contiene las definiciones y las guías prácticas necesarias para evaluar y mitigar los riesgos identificados dentro de los sistemas de TI. Su objetivo final es ayudar a las organizaciones a gestionar mejor los riesgos mediante un proceso de tres pasos: evaluación, mitigación, análisis y evaluación del riesgo [22].

2.5. Resumen, Ventajas y Desventajas

Si bien, la elección de una metodología dependerá del contexto y conocimiento del analista o equipo que realizará el trabajo, existen una serie de ventajas e inconvenientes [22][23] que se pueden poner de manifiesto, como se puede ver en la Tabla

Metodología	Ventajas	Desventajas
MAGERIT	Alcance completo en el análisis y gestión de riesgos. Está bien documentada en cuanto a recursos de información, amenazas y tipos de activos. Utiliza un completo análisis de riesgo cuantitativo y cualitativo. Es libre y no requiere autorización para su uso. Divide los activos de la organización en diferentes grupos, para identificar más riesgos y poder tomar contramedidas para evitar así cualquier riesgo. Se centra en tres objetivos: concientizar sobre la existencia de los riesgos y de la necesidad de atajarlos a tiempo, ofrecer un método sistemático para analizar tales riesgos, ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación. Permite que el proceso esté bajo control en todo momento y contempla aspectos prácticos para la realización de un análisis y una gestión de riegos efectiva.	En su modelo no involucra los procesos, recursos, ni vulnerabilidades. Posee falencias en el inventario de políticas. Se considera una metodología costosa en su aplicación
MEHARI	Para su análisis de riesgos utiliza un modelo cuantitativo y cualitativo. Es un método capaz de evaluar y lograr la disminución de riesgos en función del tipo de organización.	Se enfoca solo en los principios de integridad, confidencialidad y disponibilidad, olvidando el no repudio.

	Posee bases de datos de conocimientos con manuales, guías y herramientas que permiten realizar el análisis de riesgos cuando sea necesario. Por medio de esta metodología se detectan vulnerabilidades mediante auditorías y se analizan las situaciones de riesgo. Combina análisis y evaluación de riesgos; particularmente, se especifica un módulo de evaluación rápida y uno de evaluación detallada	La recomendación de los controles no se incluye dentro del análisis sino dentro de la gestión de los riesgos. El impacto de los riesgos se estima en el proceso de gestión y evaluación
NIST SP 800 - 30	Bajo costo relacionado con el riesgo analizado y solventado. Proporciona una guía para evaluación de riesgos de seguridad en las infraestructuras de TI. Presenta un resumen de los elementos clave de las pruebas de seguridad técnica y la evaluación con énfasis en técnicas específicas, sus beneficios, limitaciones y recomendaciones para su uso. La guía provee herramientas para la valoración y mitigación de riesgos. Asegura los sistemas informáticos que almacenan, procesan y transmiten información. Mejora la administración a partir de los resultados del análisis de riesgos.	En su modelo no tiene contemplados elementos como los procesos, los activos ni las dependencias.
CRAMM	Aplica los conceptos de manera formal, estructurada y disciplinada protegiendo los principios de seguridad y sus activos. Realiza un análisis de riesgos cualitativo y cuantitativo.	En su modelo no tiene contemplados elementos como los procesos y los recursos.

	Es aplicable a todo tipo de sistemas y redes de información y se puede utilizar en todas las etapas del ciclo de vida del sistema de información desde la planificación y viabilidad, por medio del desarrollo e implementación del mismo. Se puede usar siempre que sea necesario para identificar la seguridad y/o requisitos de contingencia para un sistema de información o de la red. Identifica y clasifica los activos de TI. Evalúa el impacto empresarial. Identifica y evalúa amenazas y vulnerabilidades, evalúa niveles de riesgo e identifica los controles requeridos. Compuesta por más de 4.000 contramedidas reunidas en grupos y subgrupos con los mismos aspectos de seguridad, incluyendo activos de software, hardware y protecciones medioambientales. Combina análisis y evaluación de riesgos	
OCTAVE	Es una metodología auto dirigida, es decir, la organización gestiona y dirige la evaluación de sus riesgosa través de un equipo multidisciplinario. Comprende los procesos de análisis y gestión de riesgos. Involucra a todo el personal de la entidad. Se considera de las más completas, ya que involucra como elementos de su modelo de análisis: procesos, activos y dependencias, recursos, vulnerabilidades, amenazas y salvaguardas.	No toma en cuenta el principio de no repudio de la información como objetivo de seguridad. Usa muchos documentos anexos para llevar a cabo el proceso de análisis de riesgos, lo que la hace tediosa, complicada de entender. Requiere de profundos conocimientos técnicos.

		No explica en forma clara la definición y determinación de los activos de información

Tabla 4 - Ventajas y Desventajas Modelos

3. BIA – Análisis de Impacto en el negocio

El análisis de impacto al negocio – BIA, es un informe que muestra consideraciones importantes para la gestión del riesgo dentro de una organización, el análisis de los costes que puede ocasionar la interrupción de un proceso crítico dentro la compañía y la estimación del tiempo que la organización puede tolerar, en caso de un incidente o desastre.

El BIA forma parte esencial en la construcción del Plan de Continuidad de Negocios y es una guía que permite identificar operaciones y servicios críticos dentro de la organización.

El soporte del BIA permite identificar qué activos de información (software,hardware, procesos, personas y normatividad) están en riesgo, una vez se haya elaborado este documento, la compañía está en la potestad de clasificar los procesos del negocio de acuerdo a su criticidad, estableciendo un orden o escala de prioridad para la ejecución de actividades que se requieran en la recuperación o restablecimiento del proceso ante alguna eventualidad o desastre que le impida operar normalmente [24].

El BIA y el análisis de riesgos evalúan dos conjuntos de datos completamente diferentes. El BIA evalúa el impacto de no efectuar un proceso de negocio en particular en el tiempo y mide los impactos cuantitativos y cualitativos de no efectuar dicho proceso. El análisis de riesgos evalúa los riesgos que podrían afectar las instalaciones, la magnitud del impacto y la probabilidad relativa de ocurrencia. Se trata de dos conjuntos de datos de información diferentes, pero cuando se combinan, pueden contar una historia de gran valor acerca de lo rápido que una interrupción puede afectar un negocio, donde tendrá el impacto más grave, la rapidez con que se producirá el impacto, y en qué orden de magnitud [25].

Las fases [24] utilizadas para elaborar el BIA, tiene en cuenta las siguientes etapas:

- Identificación de los procesos críticos e importantes que permitan la continuidad y estabilidad de la organización en el momento de una interrupción, asignado niveles de prioridad e identificando los de mayor y menor impacto.
- Valoración de los impactos que afecten los aspectos financieros, cliente interno, cliente externo, legales, regulatorio, imagen y reputación, humano y de infraestructura, en el momento de presentarse una interrupción sobre los procesos considerados de alta prioridad.
- Determinación de los tiempos objetivos de recuperación para cada uno de los procesos en evaluación, identificando la información necesaria para reestablecer el proceso, así

como la capacidad de reconstruirse automática o manualmente, en caso de ser necesario.

- Establecer la prioridad de aquellos procesos que se recuperarán, clasificándolos lo de acuerdo a la criticidad, de tal manera que sea posible seleccionar cuales procesos serán recuperados y restaurados ante una situación crítica, es decir establecimiento de la secuencia de recuperación de procesos seleccionados.
- Determinación de los recursos asociados a los procesos críticos de tal manera que se pueda definir la secuencia de recuperación de dichos recursos de acuerdo a la prioridad de los procesos y tiempos establecidos de recuperación. En la figura se describe cada una de las etapas o actividades que se implementan para realizar un análisis de impacto al negocio.

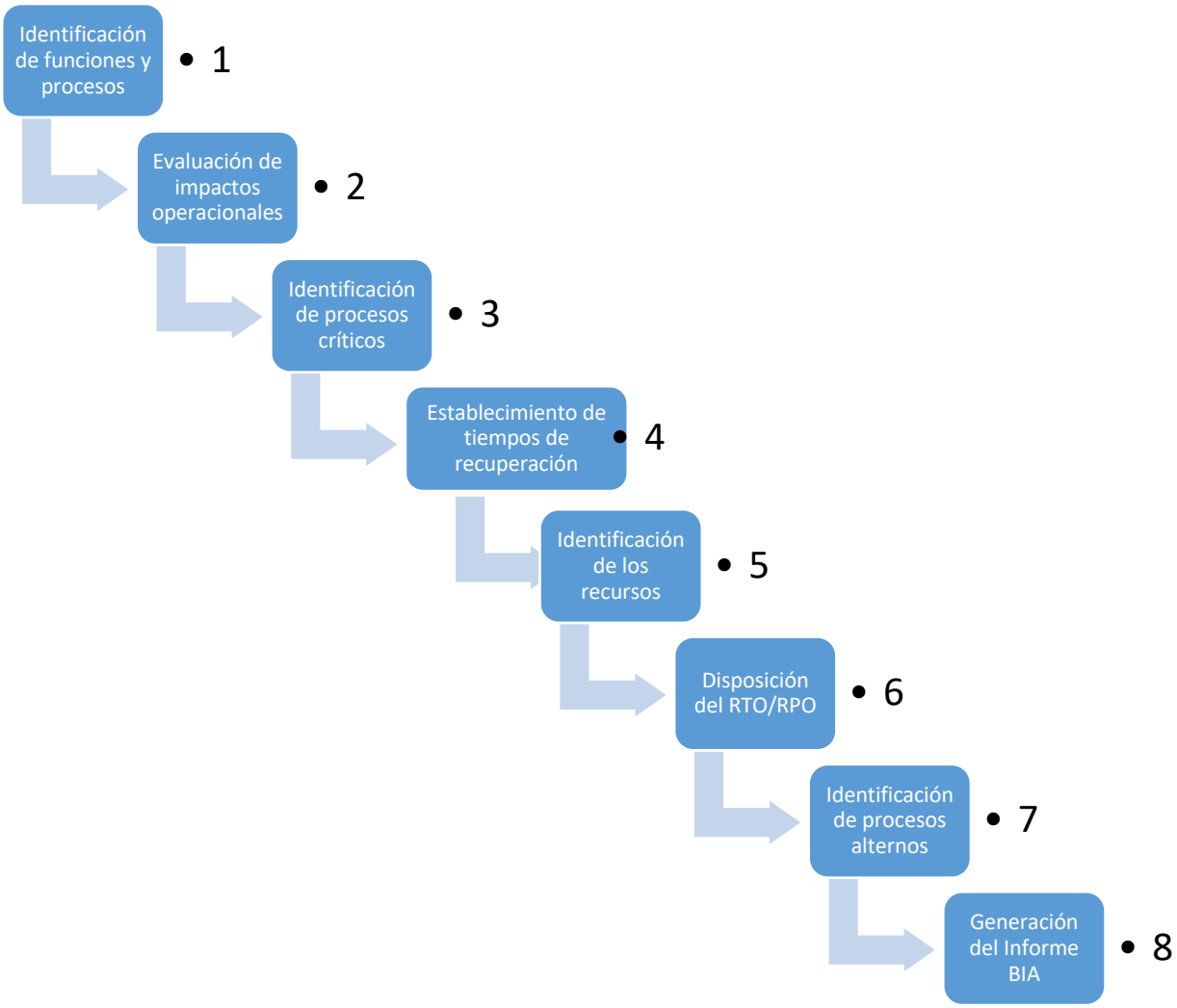

Figura 11 - Etapas BIA

Requerimientos de tiempo de recuperación

Como parte del plan de continuidad del negocio de una organización, es importante poder definir y entender los requerimientos de tiempo necesarios para recuperar a las entidades de servicios que han sido interrumpidos por diferentes motivos dentro de la organización; estos requerimientos obedecen a varios componentes que hacen referencia concreta al tiempo disponible en la cual una organización puede recuperarse oportuna y ordenadamente a las interrupciones en los servicios e infraestructuras de TI. Los componentes se describen a continuación:

- MTD (Maximun Tolerable Downtime) o Tiempo Máximo de Inactividad Tolerable. Espacio de tiempo durante el cual un proceso puede estar inoperante hasta que la empresa empiece a tener pérdidas y colapse.
- RTO (Recovery Time Objective) o Tiempo de Recuperación Objetivo. Es el tiempo transcurrido entre una interrupción y la recuperación del servicio. Indica el tiempo disponible para recuperar sistemas y recursos interrumpidos.
- RPO (Recovery Point Objective) o Punto de Recuperación Objetivo. Es el rango de tolerancia que la entidad puede tener sobre la pérdida de datos y el evento de desastre.
- WRT (Work Recovery Time): Es el tiempo invertido en buscar datos perdidos y la realización de reparaciones. Se calcula como el tiempo entre la recuperación del sistema y la normalización de los procesos.

Fases del BIA

Identificación de procesos críticos: consiste en identificar los procesos en base al impacto que operacional en la entidad u organización, suele categorizarse en tres niveles: Crítico para el Negocio, No crítico pero parte del mismo y la operación no es parte integral.

Valorar el impacto operativo y financiero: permite obtener la estimación del impacto en el negocio de la indisponibilidad del sistema y las implicaciones operacionales asociadas.

Establecimiento de Tiempos de Recuperación: Una vez identificados los procesos críticos del negocio, función que hace parte del análisis de los impactos operacionales, se procede a identificar el MTD, que corresponde al tiempo máximo de inactividad que puede tolerar una organización antes de colapsar y se hace la clasificación a fin de priorizar la recuperación del proceso (servicio). Esto quiere decir que si por ejemplo un proceso tiene un periodo máximo de tiempo de inactividad (MTD) de un (1) día, este debe tener mayor prioridad para iniciar el evento

de recuperación, en razón al poco tiempo de tolerancia de la inactividad, frente a otros que tienen mayor tolerancia [26].

Identificación de Recursos: las actividades de negocio críticas puede ser que se desarrollen sobre sistemas TI que por una relación directa será necesario identificar como recursos críticos.

Disposición los tiempos objetivos y de recuperación:

- RTO: Tiempo de Recuperación Objetivo: Asociado con la restauración de los recursos que han sido alterados de las Tecnologías de la Información comprende el tiempo disponible para recuperar recursos alterados.
  Adicionalmente, se aplica el WRT, es decir el tiempo que es requerido para completar el trabajo que ha estado interrumpido con el propósito de volverlo a la normalidad.
- RPO: Punto de Recuperación Objetivo: Este punto es importante para determinar por cada uno de los procesos críticos (servicios), el rango de tolerancia que una Entidad puede tener sobre la pérdida de información y el evento de desastre [26].

Identificación de los procesos alternos: consiste en la identificación de los métodos alternativos que de manera temporal permiten superar la crisis que ha generado la interrupción.

Generación del informe de impacto en el negocio: realización del documento que muestra los resultados del análisis realizado.

4. Análisis del Impacto en los Modelos

Las diferentes metodologías expuestas en el punto anterior tienen en común, entre otros aspectos, la definición de Riesgo y su cálculo. No obstante, la valoración del impacto suele estar calibrada mediante diferentes niveles o escalas que determinan el resultado final de los análisis de riesgos.

La valoración del impacto, en general, viene determinada del siguiente modo [21]:

- Alto: La ejecución de una vulnerabilidad (1) puede causar una alta pérdida económica de los principales activos tangibles o recursos; (2) puede significativamente violar, dañar, impedir alcanzar la misión de la organización, reputación, o intereses; o (3) puede causar la muerte humana o lesiones graves.
- Medio: La ejecución de la vulnerabilidad (1) puede resultar en la pérdida económica de activos de la empresa o recursos; (2) puede violar, dañar, o impedir alcanzar la misión de la organización, reputación, o intereses; o (3) puede resultar en lesiones personales.
- Bajo: La ejecución de la vulnerabilidad (1) puede causar la pérdida de algunos recursos o activos tangibles o (2) puede evidenciar un daño en la misión de la organización, reputación o intereses

En Octave el valor del impacto se mide como una medida cualitativa de estos tres niveles descritos.

Existen valoraciones de 5 niveles que permiten cuantificar el riesgo de un modo mas detallado y que pueden estar calculadas en función de la probabilidad del evento [27]:

- Muy Alto: Son los riesgos sobre los que la organización debe prestar la máxima atención.
- Alto: Estos riesgos tienen una alta probabilidad de ocurrencia o un impacto significativo
- Medio: Existe una posibilidad media de que los riesgos parezcan con un impacto notable.
- Bajo: Estos riesgos pueden ocurrir en algunas situaciones y tienen un impacto de bajo a medio.
- Insignificante: Existen riesgos con baja probabilidad de ocurrencia y bajo impacto. Por lo tanto, puede ser descuidado.

En Magerit, se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos y la degradación que causan

las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema se centre en la información que maneja y los servicios que presta; pero las amenazas suelen materializarse en los medios [28].

Adicionalmente, Magerit, define el impacto acumulado e Impacto repercutido que permiten calibrar de un modo mas ajustado el riesgo.

El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada. El impacto es tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo. El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado. El impacto acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

- El Impacto repercutido es el calculado sobre un activo teniendo en cuenta su valor propio y las amenazas a que están expuestos los activos de los que depende.
- El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada.
- El impacto es tanto mayor cuanto mayor es el valor propio de un activo.
- El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.
- El impacto es tanto mayor cuanto mayor sea la dependencia del activo atacado.
- El impacto repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información.

En Mehari, la definición de impacto intrínseco de un escenario es la evaluación de las consecuencias de la materialización del evento de riesgo. Ocurre, independientemente de las medidas de seguridad adoptadas. La valoración se realiza mediante una tabla denominada de impacto intrínseco. Adicionalmente, la base de conocimiento de la metodología pone a disposición de los usuarios una tabla que puede ser utilizada de referencia en los procesos de evaluación [29].

Cramm, lleva a cabo una valoración de los activos que en caso de impacto compara con unas guías o tablas internas (por ejemplo, "pérdidas financieras / interrupción de actividades")

proporcionadas por la metodología para obtener un valor la escala de 1 a 10. El rango de valores es personalizable (por ejemplo, "1" para “pérdidas de $ 1000 o menos”, “2” para “pérdidas de entre $ 1000 y $ 10,000”, etc.) [30]. En este caso, la dificultad radica en la valoración correcta de los propietarios de los activos, una subestimación o sobrevaloración de los mismos puede desvirtuar el impacto asociado.

En NIST SP 800:30 el nivel de impacto es la magnitud del daño que puede ser esperado como resultado de las consecuencias de un acceso no autorizado que llevara a cabo revelación, modificación o destrucción de la información o perdida de disponibilidad de los sistemas [31].

La metodología documenta 5 niveles de impacto en su apéndice que pueden servir como punto de entrada y guía que debe ser ajustada a las condiciones específicas de cada organización. Estos niveles semi-cuantitativos, están categorizados del siguiente modo:

- Muy Alto: 10 (100-96) Severo
- Alto: 8 (95-80) Severo o Catastrófico
- Moderado: 5 (79-21) Serio
- Bajo: 2 (20-5) Limitado
- Muy Bajo 0 (4 -0) Despreciable

El análisis de impacto en el negocio (BIA) es una parte clave del proceso de continuidad del negocio, que analiza funciones de negocio de misión crítica, e identifica y cuantifica el impacto que podría tener en la organización la pérdida de esas funciones operativas o financieras.

Con los riesgos existentes identificados para la organización el siguiente paso es determinar como esos riesgos afectan a las operaciones. Mediante cuestionarios y entrevistas con los responsables de las diferentes funciones del negocio se identifica toda la información que ayudará a determinar la criticidad e importancia de los procesos llevados a cabo por las unidades de negocio. Existen variedad de información que se requerirá al personal de la empresa, pero en el contexto del presente trabajo son de especial relevancia los siguientes elementos:

- Impacto cuantitativo: La cantidad financiera asociada al proceso, como puede ser por ejemplo, los ingresos anuales obtenidos por el mismo.
- Impacto cualitativo: El impacto no financiero para la organización, como puede ser la perdida reputacional o pérdida de clientes asociadas al proceso.

5. Antecedentes

Las diferentes metodologías de riesgos descritas en el trabajo contemplan, en general, una valoración semi-cuantitativa o mixta para el cálculo de impacto. No se encuentre mucha literatura que describa en detalle los pasos para determinar de un modo sistemático dicho cálculo, no obstante el autor Ming-Chang Lee en su *paper* denominado "*Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method" [32]* desarrolla un análisis de riesgos cuantitativo que nos servirá de referencia para analizar el impacto y que detallamos a continuación.

La aproximación que presenta cuenta de dos elementos básicos: la probabilidad de que un evento se materialice y la pérdida que puede ser incurrida. Adicionalmente utiliza elementos como son: Perdida Anual Esperada (ALE del inglés *Annual Loss Expected*), valor de salvaguarda y Retorno de la inversión (ROI).

(1) Cálculo del valor de riesgo:

$$R = p * W \; y \; p = F * V \qquad (1)$$

Donde:

R – Valor de Riesgo

p – El número de incidentes probables que puedan causar pérdida de valor de los activos en el periodo definido.

W – El valor de la pérdida del activo en un único incidente

F – Frecuencia de ocurrencia de la amenaza

V - Es la medida de probabilidad de uso de susceptibilidad especificada por una amenaza dada

(2) Annual Loss Expected (ALE)

Determinado por el producto de la probabilidad de ocurrencia de un evento que tiene impacto negativo sobre las tecnologías de la información y el valor de las pérdidas asociadas.

$$ALE = Probabilidad \; x \; Valor \; de \; Pérdida$$

$$ALE = \sum_{i=1}^{n} (I(O_i) * F_i) \qquad (2)$$

Donde:

$\{O_1, O_2, \ldots, O_n\}$ – Conjunto de efectos negativos de un evento.

$I(O_i)$ – Valor resultante de la pérdida de un evento

F_i – Frecuencia de un evento

(3) Cálculo del valor de salvaguarda

$$VS = (ALE\ Antes - ALE\ Después) - CAC \qquad (3)$$

ALE Antes – Pérdida anual esperada antes de aplicar cualquier contramedida o elemento que mitigue el riesgo identificado

ALE Después – Pérdida anual esperada después de aplicar cualquier contramedida o elemento que mitigue el riesgo identificado

CAC – Coste anual de la contramedida aplicada

(4) Retorno de la Inversión

Evaluación que compara los beneficios con respecto los costes.

$$ROI = \frac{B}{C} \qquad (4)$$

Donde:

B – Beneficios, B = S + Ganancias_Potenciales

S – Reducción de costes de ALE, S = ALE (línea base) – ALE (con la nueva protección)

Ganancias_Potenciales – Beneficios que podrían obtenerse en el caso de que se reaprovechara la protección en otras empresas, unidades, etc.

C – Costes de protección

En el modelo anterior el cálculo del impacto esta establecido en la variable W de la fórmula (1) en el que se contemplan aspectos como la pérdida anual esperada y el ROI. Esté calculo acerca la valoración de impacto en el análisis de riesgos a como se calcula en el análisis de impacto en

el negocio (BIA). Si bien, esta estimación es robusta y mediante la formulación establecida contempla todos los efectos negativos de un evento, consideramos necesario que se acoten con más detalle dichos efectos para que el usuario que realice el análisis de riesgos disponga de un modo más objetivo para la obtención del impacto.

Del análisis de las diferentes metodologías de riesgos junto con el modelo anterior fijaremos las variables o aspectos mas relevantes que pueden ayudar a calcular de un modo mas ajustado el impacto ante un posible evento de riesgo.

6. Modelo Propuesto

Los análisis de riesgos desarrollados en el presente trabajo muestran una valoración del impacto semi-cuantitativa o cualitativa que si bien están aceptados como modelos válidos incorporan un factor subjetivo a la estimación que puede desvirtuar en cierta medida el análisis de riesgos realizado.

Sistematizar esta valoración de modo que quede lo mas alineada posible a las métricas de las empresas y que permita obtener unos resultados mas robustos es el objetivo del modelo que proponemos.

En este sentido vamos a desarrollar la ecuación (2) del trabajo de Ming-Chang Lee que en su *paper* denominado "*Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method" [32]* desarrolla un análisis de riesgos cuantitativo que nos servirá de referencia y que se ha detallado en la sección de antecedentes.

La fórmula principal del trabajo obtiene el sumatorio de los impactos negativos en importes monetarios supeditados a la existencia o frecuencia de dicho evento:

$$ALE = \sum_{i=1}^{n} (I(O_i) * F_i) \qquad (5)$$

Donde:

$\{O_1, O_2, \ldots, O_n\}$ – Conjunto de efectos negativos de un evento.

$I(O_i)$ – Valor resultante de la pérdida de un evento

F_i – Frecuencia de un evento

En dicha formulación no se especifican con detalle que elementos o efectos negativos se deben contemplar para realizar el cálculo de la pérdida. Así mismo las metodologías descritas dejan en manos de los analistas de riesgos la determinación e identificación de dichos eventos.

Estimar que variables son las que se tienen que incluir en el cálculo es parte del proceso de objetivación y propósito del trabajo realizado. Así, consideramos que el conjunto de efectos negativos de un evento $\{O_1, O_2, \ldots, O_n\}$ que se deberán contemplar incluyen aspectos relacionados con el negocio, la operación, tecnología y reputación. Si bien, este último tienen un carácter cualitativo que en determinados ámbitos podría suponer elevadas pérdidas para las empresas.

El negocio es el elemento esencial y mas sensible de la organización, realmente no se concibe una empresa sin el mismo, con lo que se convierte el aspecto mas relevante de protección. Tanto la operación como la tecnología son ámbitos sobre los que el negocio se sustenta y soporta. Las áreas tecnológicas hoy en día dan cobertura a gran parte de los procesos de operación y quedan estrechamente relacionado con el negocio, con lo que la vinculación entre las mismas implica que exista una dependencia directa entre los impactos asociados.

Los primeros efectos negativos que vamos a contemplar y que vienen establecidos por el BIA, y por ende relacionadas con el negocio, son lo que denominaremos Impacto Transaccional e Impacto de Oportunidad.

El impacto transaccional valora el impacto que supone para la organización el no poder llevar a cabo una determinada operación. Supongamos, por ejemplo una entidad financiera que su sistema de transacciones dejara de funcionar y no pudiera recibir transferencias de clientes. Este valor se estima como volumen de operaciones no realizadas e importes no recibidos en el periodo. Estas operaciones que suponen un benefició en su modo habitual en caso de no poder realizarse computarán como pérdida.

El impacto de oportunidad contempla aspectos negativos relacionados con el mantenimiento y mejora del proceso que deja de funcionar. En el ejemplo anterior, si el sistema de transacciones deja de funcionar, es altamente probable que no se puedan dar de alta nuevos clientes o modificar las comisiones de las transferencias. Esto son impactos colaterales que tienen que ser contemplados. Para poder identificar relación entre los procesos de negocio se considera necesario disponer de una matriz de dependencia que ayudará a identificar los impactos colaterales.

Los impactos anteriores están relacionados con el BIA, pero existen otros criterios a tener en cuenta adicionales a los relacionados directamente con la función de negocio y que viene del análisis riesgos [33] .

Costes de reparación o sustitución: contempla los gastos necesarios para restablecer los dispositivos físicos, sustitución de los mismos y actividades dirigidas a esta finalidad. Este es un impacto directamente relacionado con la tecnología, deberán incluir tanto los costes de los trabajos realizados en la restauración de los dispositivos como los trabajos personales dirigidos con tal fin.

Perdida del Activo: coste de la pérdida económica del activo. Según la definición del plan contable se deberían contemplar las pérdidas producidas en la enajenación de inmovilizado

intangible, material o las inversiones inmobiliarias o por su baja del activo, como consecuencia de pérdidas irreversibles de dichos activos.

Pérdida reputacional: costes relacionados con la imagen y reputación de la organización. La marca es un elemento intangible que se ha convertido en uno de los aspectos que las organizaciones protegen con vehemencia. La proliferación de las redes sociales da visibilidad de un modo exponencial a las empresas lo que les permite llegar a gran conjunto de público objetivo. Esta situación garantiza el éxito de campañas de marketing pero a su vez implica que cualquier deterioro de la imagen debido a factores internos como externos se expanda con gran rapidez entre los consumidores.

Infracciones legales o ruptura de condiciones contractuales: el impacto económico de sanciones e indemnizaciones son más habituales en los entornos regulados como el Bancario, Asegurador o Energético. Por ejemplo, en el Reglamento General de Protección de Datos, se indica que las sanciones impuestas por infracciones en materia de datos pueden llegar hasta los 20 millones de euros o el 4% del volumen de negocio global anual del ejercicio financiero anterior de la compañía infractora.

Daños personales: costes asociados a la subsanación y/o reparación de los costes personales. Por una parte deberán contemplarse los costes económicos de nuevas contrataciones, incluyendo formación de los recursos, prestaciones y compensaciones tanto al trabajador como y por otra los pagos adicionales a los diferentes estamentos gubernamentales que gestionan las relaciones laborales.

Los impactos identificados anteriormente se pueden calcular en importes monetarios lo que permite ser entendido desde una perspectiva de negocio y es extrapolable a cualquier sector o país, no obstante, el modelo permite una valoración semi-cuantativa que para cada uno de los impactos se pueden utilizar las categorías definidas en la metodología de riesgos que se esté utilizando.

Las diferentes categorías de los impactos anteriores han sido determinadas por su importancia o preocupación de los riesgos de las empresas. Así, en el informe *Global Risk Management Survey* [34] de 2017 podemos ver la preocupación por los riesgos por importancia para los empresarios. A la tabla hemos añadido la columna que indica si dicho riesgo queda contemplado en los impactos que utiliza el modelo, como se puede ver en la Tabla 5.

Descripción	Incluido en Modelo
Daño a la reputación / marca	Si
Desaceleración económica / recuperación lenta	No Aplica
Aumento de la competencia	No Aplica
Cambios reglamentarios / legislativos	Si
Delito cibernético / hacking / virus / códigos maliciosos	Si
No innovar / satisfacer las necesidades de los clientes	Si
Faltas en la atracción o retención de los mejores talentos	No Aplica
Interrupción del negocio	Si
Riesgo político / incertidumbre	No Aplica
Responsabilidad civil	Parcial

Tabla 5 - Riesgos Relevantes 2017

Puesto que las metodologías utilizadas son las relacionadas con los sistemas de información los ámbitos externos relacionados con desaceleración económica, aumento de la competencia, retención de talentos y riesgo político no aplican directamente en el cálculo.

Así con todo lo anterior tenemos como resultado que para la valoración del impacto para un evento particular n será la suma de la pérdida económica para todos los efectos identificados por la frecuencia del evento:

$$IMP_n = \mathrm{I}(\mathrm{I_t}) + I(\mathrm{I_o}) + I(\mathrm{C_r}) + I(\mathrm{P_a}) + I(\mathrm{P_r}) + I(\mathrm{I_l}) + I(\mathrm{D_p}) \qquad (6)$$

Donde:

$\mathrm{I}(\mathrm{I_t})$ – Impacto transaccional

$\mathrm{I}(\mathrm{I_o})$ – Impacto de oportunidad

$\mathrm{I}(\mathrm{C_r})$ – Costes de reparación

$\mathrm{I}(\mathrm{P_a})$ – Costes de la pérdida del activo

$\mathrm{I}(\mathrm{P_r})$ – Costes de la pérdida reputacional

$\mathrm{I}(\mathrm{I_l})$ – Coste legal por sanciones e indemnizaciones

$\mathrm{I}(\mathrm{D_p})$ – Coste por daños personales

En el caso en el que se opte por un análisis semi-cuantitativo, es decir sin cálculos monetarios, la fórmula utilizada puede realizarse o bien eligiendo el máximo de los impactos o mediante el cálculo de la media de los diferentes valores:

Máximo:

$$IMP_n = max(\mathrm{I}(\mathrm{I_t}), I(\mathrm{I_o}), I(\mathrm{C_r}), I(\mathrm{P_a}), I(\mathrm{P_r}), I(\mathrm{I_l}), I(\mathrm{D_p})) \quad (7)$$

Media:

$$IMP_n = \frac{\mathrm{I}(\mathrm{I_t}) + I(\mathrm{I_o}) + I(\mathrm{C_r}) + I(\mathrm{P_a}) + I(\mathrm{P_r}) + I(\mathrm{I_l}) + I(\mathrm{D_p})}{6} \quad (8)$$

Por tanto, mediante la cuantificación del impacto, el cálculo del riesgo queda:

$$R = p * IMP \quad (9)$$

Donde:

R – Valor de Riesgo

p – El número de incidentes probables que puedan causar pérdida de valor de los activos en el periodo definido.

IMP – La cuantificación objetiva del impacto.

Las variables que no pueden ser calculadas se establecen con valor 0. El cálculo final del impacto se puede realizar de diferentes modos, en el caso de que optemos por la opción semi-cuantitativa elegiremos el máximo de los valores. También podemos seleccionar la media de los impactos que con categorización distinta de 0, no obstante, recomendamos el uso del máximo que contempla el peor escenario sobre el evento de riesgo.

En el caso de que optemos por la opción cuantitativa, el resultado será la suma de los importes monetarios obtenidos que adicionalmente puede ser categorizado en niveles en comparación con las tablas financieras que disponga la organización que se esté analizando. Así con los datos numéricos obtenidos se podría obtener una tabla [33] del siguiente tipo:

Rango de Impacto	Descripción	Cuantificación del Impacto
5	Catastrófico	>6% del presupuesto
4	Desastroso	6% del presupuesto
3	Serio	2% del presupuesto
2	Menor	1% del presupuesto
1	Insignificante	<0,5% del presupuesto

Tabla 6. Categorización de Impacto

El modeló presentado permite una definición objetiva del impacto sin tener en cuenta las salvaguardas, no obstante, para cada uno de los impactos habría que determinar la minoración por la efectividad de los elementos mitigantes lo que aportaría el calculo objetivo post controles mitigatorios.

Contraste y Ejemplo de Uso

De la web de INCIBE hemos obtenido el resultado de un ejemplo simplificado de análisis de riesgos [35]:

ANÁLISIS DE RIESGOS				
ACTIVO	**AMENAZA**	**PROB**	**IMPACTO**	**RIESGO**
Servidor 01 (Contabi)	Fuga de información	2	3	6
Servidor 01 (Contabi)	Degradación de los soportes	1	3	3
Router Wifi (Clientes)	Caída del sistema por sobrecarga	1	2	2
Router Wifi (Clientes)	Denegación de servicio	2	1	2
Servidor 02 (Web)	Denegación de servicio	3	2	6
Servidor 02 (Web)	Corte del suministro eléctrico	1	2	2

Tabla 7 - Ejemplo sencillo análisis de riesgos

La categorización del impacto la realizan del siguiente modo:

- Bajo (1) El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
- Medio (2) El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
- Alto (3) El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Tanto la descripción de “consecuencia no relevante” o “reseñable” tienen una connotación subjetiva que podría distorsionar el análisis de riesgos.

Con el modelo propuesto, la estimación de las variables de impacto y utilizando los mismos niveles de impacto establecidos en el ejemplo, el análisis quedaría del siguiente modo:

ACTIVO	AMENAZA	It	Io	Cr	Pa	Pr	Ii	Dp	Media	Máximo
Servidor 01	Fuga de información	0	0	2	0	2	3	0	2,33	3
Servidor 01	Degradación de los soportes	3	3	2	2	1	0	0	2,2	3
Router Wifi	Caída del sistema por sobrecarga	2	2	2	0	2	0	0	2	2
Router Wifi	Denegación de servicio	2	2	1	0	2	0	0	1,75	2
Servidor 02	Denegación de servicio	2	0	1	0	3	1	0	1,75	3
Servidor 02	Corte del suministro eléctrico	2	0	0	0	2	0	0	2	2

Tabla 8 - Ejemplo aplicación del modelo

Donde:

I_t – Impacto transaccional

I_o – Impacto de oportunidad

C_r – Costes de reparación

P_a – Costes de la pérdida del activo

P_r – Costes de la pérdida reputacional

I_l – Coste legal por sanciones e indemnizaciones

D_p – Coste por daños personales

Podemos observar como para un mismo activo y diferentes amenazas, como en el Servidor 01, cuando elegimos el máximo de los impactos como resultado el valor es el mismo que en el análisis de riesgos estándar. Cuando realizamos la media de los impactos obtenemos pequeñas diferencias, que si bien pueden parecer mínimas, nos ayudan a definir la estrategia y plan de acción sobre los activos de la organización.

Se puede ver también el efecto de las variables como el impacto reputacional e impacto de oportunidad, que pueden pasar desapercibidas para un analista no experimentado o con determinado perfil tecnológico. En el caso del Servidor 02 vinculado a un servicio para clientes la denegación de servicio tiene un impacto reputacional que debe ser tenido en cuenta y que queda claramente reflejado en el modelo.

En el caso de que se dispusiera de cálculos económicos provenientes por ejemplo del BIA las categorías no tendrían sentido dejando lugar a la suma monetaria de los impactos. Si bien, es

mucho mas detallado el análisis cuantitativo requiere de cierta experiencia y conocimiento riguroso de la organización en la que se está trabajando.

7. Conclusiones y trabajo futuro

En el presente trabajo hemos podido revisara como las diferentes metodologías llevan a cabo el calculo del impacto mediante las diferentes perspectivas tanto cualitativas como cuantitativas.

Los enfoques cualitativos permiten agilizar el desarrollo de los análisis lo que mejora los tiempos de desarrollo y reduce costes. Así mismo permiten obtener una visión de los grandes riesgos de un modo robusto y ajustado. Como contrapartida, se identifican carencias relacionadas con el detalle fino o granular de los riesgos. La estratificación de los cálculos en categorías puede crear un sesgo en los cálculos que distorsione la foto global del análisis.

Por este motivo, los cálculos cuantitativos permiten afinar con mas exactitud los valores numéricos del análisis. Como contrapartida, la valoración requerirá mas tiempo y cierta experiencia del analista que lo realice.

Los perfiles de carácter tecnológico, en general, presentan recorrido de mejora en cuanto a terminología financiera y cálculo de costes económicos. Así mismo, la visión global de los aspectos operacionales y gerenciales de las organizaciones no suele ser uno de los ámbitos de fortaleza de este colectivo.

Así pues, el establecer las diferentes variables de costes asociados a eventos de pérdida presentados en este trabajo, permite objetivizar el cálculo de impacto para personal no financiero.

El cálculo obtenido, si bien, es un valor numérico que *per se* no es descriptivo permite combinarse con modelos cualitativos que enriquezcan los datos obtenidos. La combinación de la valoración cuantitativa junto la cualitativa es la mas recomendable en cuanto a la cuantificación del impacto. Estos análisis de carácter híbrido son soportados por la mayoría de las metodologías actuales.

En cuanto a la tendencia actual en modelos de análisis de riesgos, se dirigen a automatizar el cálculo de impacto al igual que se hace en el cálculo de probabilidades. En este segundo caso, mediante el análisis de logs y eventos en los SIEM (Información de seguridad y gestión de eventos) se puede determinar la probabilidad de que un evento se produzca. En el caso del cálculo de impactos, mediante el registro de eventos de pérdida, se puede llevar a cabo el mismo análisis que el de probabilidades.

La madurez en cuanto a la gestión de riesgo determinará hasta que punto es posible utilizar datos históricos registrados para realizar predicciones y proyecciones sobre el cálculo de impacto.

Tanto el uso de BigData como la adopción general de técnicas de inteligencia artificial permitirá predecir de un modo automático, ajustado y rápido dicho cálculo utilizando los repositorios de información sobre eventos de pérdida.

Por este motivo, consideramos que los trabajos futuros sobre análisis de riesgos deberían centrarse en el análisis de información mediante las técnicas comentadas. Así mismo, la existencia de una base de datos común pública y abierta permitiría una calibración mas adecuada de los cálculos.

Referencias

[1] www.elmundo.com, «La crisis financiera: ¿un cisne negro?», *www.elmundo.com*. [En línea]. Disponible en: https://www.elmundo.com/portal/opinion/columnistas/la_crisis_financiera_un_cisne_negro.php#.XHa01ZNKhQI. [Accedido: 27-feb-2019].

[2] E. C. Bank, «La política monetaria del BCE durante la crisis», *European Central Bank*. [En línea]. Disponible en: https://www.ecb.europa.eu/press/key/date/2011/html/sp111021_1.es.html. [Accedido: 27-feb-2019].

[3] «(PDF) Directrices sobre la evaluación del riesgo de TIC en el marco del

proceso de revisión y evaluación supervisora (PRES)». [En línea]. Disponible en: https://eba.europa.eu/documents/10180/1954038/Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29_ES.pdf/0d081451-67d1-4f53-854e-f1b74d5b8e9e. [Accedido: 01-mar-2019].

[4] E. C. Bank, «Risk assessment», *European Central Bank - Banking Supervision*. [En línea]. Disponible en: https://www.bankingsupervision.europa.eu/banking/priorities/risk_assessment/html/index.es.html. [Accedido: 27-feb-2019].

[5] «¡Fácil y sencillo! Análisis de riesgos en 6 pasos», *INCIBE*, 16-ene-2017. [En línea]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo. [Accedido: 23-feb-2019].

[6] «Metodología». [En línea]. Disponible en: https://www.ccn-cert.cni.es/soluciones-seguridad/ear-pilar/metodologia.html. [Accedido: 01-mar-2019].

[7] «AN INTRODUCTION TO INFORMATION SYSTEM RISK MANAGEMENT 1 1 Preface». [En línea]. Disponible en: https://www.coursehero.com/file/pu46g5/AN-INTRODUCTION-TO-INFORMATION-SYSTEM-RISK-MANAGEMENT-May-31-2006-1-1-Preface/. [Accedido: 01-mar-2019].

[8] T. Aven, «Risk assessment and risk management: Review of recent advances on their foundation», *Eur. J. Oper. Res.*, vol. 253, n.º 1, pp. 1-13, ago. 2016.

[9] J. G. M. P. de León, *Introducción al análisis de riesgos*. Editorial Limusa, 2007.

[10] F. Khan, S. Rathnayaka, y S. Ahmed, «Methods and models in process safety and risk

management: Past, present and future», *Process Saf. Environ. Prot.*, vol. 98, pp. 116-147, nov. 2015.

[11] G. E. Apostolakis, «How Useful Is Quantitative Risk Assessment?», *Risk Anal.*, vol. 24, n.º 3, pp. 515-520, jun. 2004.

[12] «(PDF) Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method», *ResearchGate*. [En línea]. Disponible en: https://www.researchgate.net/publication/260480809_Information_Security_Risk_Analysis_Methods_and_Research_Trends_AHP_and_Fuzzy_Comprehensive_Method. [Accedido: 01-mar-2019].

[13] R. Gómez, D. H. Pérez, Y. Donoso, y A. Herrera, «Metodología y gobierno de la gestión de riesgos de tecnologías de la información», *Rev. Ing.*, n.º 31, pp. 109-118, 2010.

[14] Abril Estupiñan, A., Pulido, J., & Bohada Jaime, J. (2013). Análisis de riesgos en seguridad de la información. Ciencia, Innovación Y Tecnología, 1, 40-53. Recuperado a partir de https://www.jdc.edu.co/revistas/index.php/rciyt/article/view/121

[15] «(PDF) Introducing OCTAVE Allegro: Improving the Information Security Risk

Assessment Process" Caralli et al. - 2007 [En linea]. Disponible en: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf [Accedido: 01-mar-2019].

[16] «Mehari». [En línea]. Disponible en: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_mehari.html. [Accedido: 19-abr-2019].

[17] «(PDF) MEHARI-2010-Introduccion», p. 15, 2010. [En linea]. Disponible en: http://meharipedia.x10host.com/wp/wp-content/uploads/2016/12/MEHARI-2010-IntroduccionESP.pdf [Accedido: 19-abr-2019].

[18] «Introducción al análisis de riesgos - Metodologías (I)», *Security Art Work*, 30-mar-2012. [En línea]. Disponible en: https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/. [Accedido: 19-abr-2019].

[19] Crespo-Martínez, E., & Cordero-Torres, G. (2018). ESTUDIO COMPARATIVO ENTRE LAS METODOLOGÍAS CRAMM Y MAGERIT PARA LA GESTIÓN DE RIESGO DE TI EN LAS MPYMES. UDAAKADEM, (1), 38 - 47. Recuperado a partir de http://revistas.uazuay.edu.ec/index.php/udaakadem/article/view/129

[20] G. Stoneburner, A. Goguen, y A. Feringa, «Risk management guide for information

technology systems :: recommendations of the National Institute of Standards and Technology», National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-30, 2002.

[21] Abril Estupiñan, A., Pulido, J., & Bohada Jaime, J. (2013). Análisis de riesgos en seguridad de la información. Ciencia, Innovación Y Tecnología, 1, 40-53. Recuperado a partir de https://www.jdc.edu.co/revistas/index.php/rciyt/article/view/121 [22] H. A. Novoa y C. R. Barrera, «Metodologías para el análisis de riesgos en los sgsi», *Publicaciones E Investig.*, vol. 9, n.º 0, pp. 73-86, oct. 2015.

[23] A. Mogollon, «(PDF) Análisis Comparativo: Metodologías de análisis de Riesgos». [En línea]. Disponible en: https://dsi.face.ubiobio.cl/sbravo/1-AUDINF/MAGERIT%20COMPARACION.pdf [Accedido: 23-abr-2019].

[24] P. A. D. Montaña, O. C. M. Martínez, y F. V. S. Sánchez, «ELABORACIÓN DEL ANÁLISIS DE IMPACTO AL NEGOCIO (BIA) COMO PARTE FUNDAMENTAL DEL PLAN DE CONTINUIDAD DE NEGOCIO DE LA CADENA RADIAL», p. 135.

[25] «¿Cuál es más importante? (BIA o RA)». [En línea]. Disponible en: https://blog.segu-info.com.ar/2012/08/cual-es-mas-importante-bia-o-ra.html [Accedido: 10-abr-2019].

[26] « (PDF) Guía para realizar el Análisis de Impacto de Negocios BIA ». [En línea]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf [Accedido: 5-abr-2019].

[27] Vasile. “Using Probability – Impact Matrix in Analysis and Risk Assessment Projects”, Diciembre 2013, Journal of Knowledge Management, Economics and Information Technology

[28] C. Supanta, «MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información». [En línea]. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html [Accedido: 11-feb-2019].

[29] A. Syalim, Y. Hori, y K. Sakurai, *Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft’s Security Management Guide*. 2014 . IEEExplore.

[30] B. Corcoran, «A qualitative risk analysis and management tool – CRAMM», p. 13, 2002. [En línea]. Disponible en: https://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83 [Accedido: 14-ene-2019].

[31] Joint Task Force Transformation Initiative, «Guide for conducting risk assessments», National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-30r1, 2012.

[32] M.- Chang Lee, «Information Security Risk Analysis Methods and Research Trends:

AHP and Fuzzy Comprehensive Method», *Int. J. Comput. Sci. Inf. Technol.*, vol. 6, n.º 1, pp. 29-45, feb. 2014.

[33] «Gestión de Riesgos». Incibe. [En línea]. Disponible en: https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf [Accedido: 11-mar-2019].

[34] «Global Risk Management Survey [En línea]. Disponible en: https://www.aon.com/getmedia/0263427c-34f5-425d-b3e9-915a8585afd4/2017-Global-Risk-Management-Survey-Report-Executive-Summary-rev-120318.aspx [Accedido: 09-may-2019].

[35] "Modelo simplificado de análisis de riesgos" - Incibe "https://www.incibe.es/extfrontinteco/img/File/empresas/dosieres/plan_director_de_seguridad/plan_director_de_seguridad__hoja_para_el_analisis_de_riesgos.xls